

# **Joint Military Intelligence Training Center**

October 1996

## **Open Source Intelligence: Professional Handbook**





## FORWARD

1. **PURPOSE.** *Open Source Intelligence: Professional Handbook*, is published to ensure the dissemination of useful information which is vital to successful intelligence support to the military commander, and highly pertinent to law enforcement and economic intelligence operations, but which may not yet be doctrinally available.

2. **SCOPE.** This publication constitutes material that was produced under contract to the Defense Intelligence Agency, Joint Military Intelligence Training Center, by OPEN SOURCE SOLUTIONS, Inc., using copyrighted OSS Inc. materials. The material has been edited by OSS to develop a single integrated publication which can be used as both a primer and an operational guide to acquiring and exploiting open source information as part of the all-source intelligence process. Open source information is often described as the "source of first resort," and may be the *only* source available to the commander and staff when initially considering an expeditionary contingency. The information contained herein does not necessarily reflect the views, nor should any endorsement or approval be implied by the Department of Defense or the Defense Intelligence Agency, or any other government organization or authority.

3. **COPYRIGHT AND DISSEMINATION.** This publication may be reproduced without restriction by any agency of the US government. It may not be used by others without prior permission of the copyright holder, OPEN SOURCE SOLUTIONS, Inc., 11005 Langton Arms Ct, Oakton VA 22124.



# OPEN SOURCE INTELLIGENCE: PROFESSIONAL HANDBOOK 1.1

## CONTENTS

INTRODUCTION	001
--------------	-----

### Chapter 1. OVERVIEW OF OPEN SOURCES & SERVICES

Paragraph		Page
1001	Purpose of the Chapter	004
1002	Definitions	004
1003	Brief History of U.S. OSINT	005
1004	OSINT & All-Source Analysis	006
1005	Knowledge Terrain: The Information Continuum	007
1006	OSINT and The Military I	008
1007	OSINT and The Military II	009
1008	Militarily Useful OSINT: Two Examples	010
1009	Representative Open Sources I	011
1010	Representative Open Sources II	011
1011	Representative Open Services I	012
1012	Representative Open Services II	013
1013	Intelligence in the Age of Information	014
1014	Changing Role of the Analyst I	015
1015	Changing Role of the Analyst II	015
1016	Changing Role of the Analyst III	016
1017	Changing Role of the Analyst IV	016
1018	Overt Human Networks: Some First Steps	017
1019	OSINT Among Selected Allies	018
1020	OSINT in Asia	019
1021	OSINT in Europe	019
1022	OSINT Within DIA I	020
1023	OSINT Within DIA II	021
1024	OSINT Within DIA III	021
1025	OSINT and the All-Source Product	022

### Chapter 2. ACCESS: Intelligence in the Age of Information

Paragraph		Page
2001	Purpose of the Chapter	024
2002	Definitions	024
2003	New "Rules of the Game"	025

2004	Four Information Categories	026
2005	Information Value	027
2006	Open Sources	027
2007	Collection Investment Strategies	028
2008	Windows of Opportunity	029
2009	Collection Management	030
2010	Four Major Consumer Groups	031
2011	Intelligence Production	031
2012	Target Categories	032
2013	Types of Overt Human Sources	033
2014	OSINT As A Resource Saver	034
2015	National Information Strategy	035
2016	Optimizing OSINT	036

### **Chapter 3. INTERNATIONAL OPEN SOURCES AND SERVICES**

Paragraph		Page
3001	Purpose of the Chapter	037
3002	American Online Services	037
3003	Foreign Online Services	038
3004	Information Brokers	039
3005	Grey Literature	040
3006	Document Acquisition	040
3007	International Experts I	041
3008	International Experts II	042
3009	International Directories	042
3010	Jane's Information Group	043
3011	Oxford Analytica	044
3012	Eastview Publications	045
3013	SPOT Image Corporation	045
3014	Universities	046
3015	Knowledge Age	047
3016	Conclusion	048

### **Chapter 4. THE INTERNET AS A TOOL FOR ALL-SOURCE ANALYSIS**

Paragraph		Page
4001	Purpose of the Chapter	049
4002	Introduction: What Is The Internet	049
4003	Where Are We Today?	050
4004	How Representative Is The Internet?	051
4005	Lists: Versatile Low-Tech Tools	052

4006	USENET and Its Newsgroups	052
4007	Conferencing Systems	053
4008	CAUTION: Some Problem Areas	054
4009	How On-Line Communities Form	055
4010	On-Line Communities, Virtual Contacts	055
4011	Structuring Knowledge: Tools and Trends	056
4012	The World-Wide Web	057
4013	Where the Web Has Been, and Where It's Headed	058
4014	Finding Information on the Web	059
4015	"Intranetting"	059
4016	Practical Example #1: Indications and Warning (I&W)	060
4017	Practical Example #2: Cultural Context	061
4018	Practical Example #3: Basic Research	061
4019	Practical Example #4: Science and Technology Collection	062
4020	Practical Example #5: Spotting and Assessment	062
4021	Second Caution: Mischief in Cyberspace	063
4022	Putting It All Together	064
4023	Anticipating Coming Changes	065
4024	Conclusion: A Work in Progress	065

## **Chapter 5. OPEN SOURCES AND MILITARY CAPABILITIES**

Paragraph		Page
5001	Purpose of the Chapter	067
5002	Model for Integrated All-Source Analysis	067
5003	General Utility of OSINT	068
5004	Strategic Intelligence	069
5005	Operational Intelligence	070
5006	Tactical Intelligence	070
5007	Technical Intelligence	071
5008	Commercial Imagery for 1:50:000 Maps	072
5009	Commercial Imagery for Mission Rehearsal	072
5010	Order of Battle Information	072
5011	Historical and Estimative Analysis	073
5012	Networks of Experts	074
5013	Expeditionary Factors Study	075
5014	Strategic Generalizations	075
5015	Commission on Intelligence	076
5016	Conclusion	077

## **Chapter 6: Open Sources and Operational Security--The Dark Side**

<b>Paragraph</b>		<b>Page</b>
6001	Purpose of the Chapter	078
6002	General Considerations	078
6003	Open Sources and Radio Interception	079
6004	Open Sources and Telephone Interception	080
6005	Open Sources and Eavesdropping	081
6006	Open Sources and Undercover Operations	082
6007	Open Sources and Interrogations	082
6008	Open Sources and Direct Research	083
6009	Open Sources and Executions	084
6010	Open Sources and Explosives	085
6011	Open Sources and Radio Detonation of Bombs	085
6012	Open Sources and Vehicular Enhancements	086
6013	Open Sources and Tactical Communications Jamming	087
6014	Open Sources and Bank Card Forgery	087
6015	Open Sources and "Legal" Offshore Passports	088
6016	Open Sources and Offshore Corporations	089
6017	Open Sources and Choosing A Criminal Specialty	090
6018	Conclusion: The Dark Side of Open Sources	091

## **Chapter 7 CONCLUSION: COLLECTING AND PROCESSING OPEN SOURCE**

<b>Paragraph</b>		<b>Page</b>
7001	Purpose of the Chapter	092
7002	Community Open Source Program Office	092
7003	Open Source Information System	093
7004	Defense Intelligence Agency Open Source Program	094
7005	Defense Intelligence Agency Open Source Intelligence Center	094
7006	Marine Corps Intelligence Activity	095
7007	Expeditionary Factors Study	095
7008	Marine Corps Reserve	096
7009	Additional Open Source Training Opportunities	097



## APPENDICES

Appendix		Page
A	White Paper on "Open Source Intelligence: What Is It? Why Is It Important to the Military?"	099
B-1	Talking Points on "Private Enterprise Intelligence: Its Potential Contribution to National Security"	110
B-2	Complete Paper on "Private Enterprise Intelligence: Its Potential Contribution to National Security"	113
B-3	Glossary of Open Source Acronyms	145
B-4	Core Open Source References	146
C	White Paper on "ACCESS: Theory and Practice of Intelligence in the Age of Information	147
D	Concise Directory of Selected International Open Sources & Services	165
E-1	Internet: Self-Guided Tour	174
E-2	Internet: Intelligence-Oriented List of Useful Internet Sites	181
E-3	Internet: Intelligence Sites from <i>PC Magazine's</i> Top 100 Web Sites	190
E-4	Internet: How to Find an Interesting Mailinglist	193
F-1	Expeditionary Environment R&A Framework & Model 1990	201
F-2	Mission Area Factors Summary	252
G	Open Source OPSEC: Selected References and Information	302
H	Expeditionary Factors Study: List of Countries	306



## INTRODUCTION

This handbook is based almost entirely on six of the eight lessons comprising the Open Source Training Course funded by the Defense Intelligence Agency (DIA). It has been prepared by the staff of the Navy-Marine Corps Intelligence Center as a means for consolidating the course materials in a form which could be most useful to the Marine Air Ground Task Force (MAGTF). All Marines will benefit from this DIA-funded initiative, which is the first organized course of instruction on open source intelligence available in the entire U.S. Intelligence Community. This material is provided to the Fleet Marine Force as an interim measure, pending the availability, possibly in 1997 or 1998, of more formal training materials from the (U.S. Intelligence) Community Open Source Program Office.

Chapter 1, OVERVIEW OF OPEN SOURCES & SERVICES, presents a broad overview of open sources and services which are important to the all-source intelligence analyst. Included in this chapter is a definition of open source and a distinction between data, information, and intelligence; a brief discussion of the history of open source intelligence as a sub-discipline within the all-source intelligence process; a review of why open sources are important to military intelligence; examples of open sources and services which are not now commonly integrated into all-source analysis; and a discussion of open source exploitation within DIA (Defense Intelligence Agency) and in a number of allied intelligence communities. This chapter concludes with a discussion of the changing role of the analyst; and how each analyst can take specific steps to improve their personal exploitation of open sources in support of the all-source intelligence process.

Chapter 2, ACCESS: INTELLIGENCE IN THE AGE OF INFORMATION, presents a more in-depth look at why open sources are critical to the all-source analysis endeavor, and how all-source analysts can optimize their exploitation of open source information. Included in this overview is a review of definitions distinguishing between data, information, and intelligence; discussions of how the art of intelligence is changing in the face of the "information explosion", the four kinds of information categories that an all-source analysts can consider accessing, and the three elements of information value; a discussion of the nine levels of open source information; an examination of possible collection management strategies which integrate open sources into the all-source collection management task and exploit windows of opportunity in which material is available in open sources just prior to being classified or censored; discussion of the four major consumer groups and their intelligence productions needs in relation to open sources; an examination of the four "warrior classes" and how open sources apply to intelligence analysis of each; discussion of the four types of overt human sources the analyst will encounter; an examination of how open source intelligence (OSINT) can help conserve scarce classified resources, and how a national information strategy can increase the amount of open source information available to the defense intelligence community; and concluding comments on optimizing OSINT in the all-source analysis process.

Chapter 3. INTERNATIONAL OPEN SOURCES AND SERVICES, provides an orientation to international open sources and services which are available to the all-source analyst. Although much of the open source world is not yet easily accessible to analysts because of security and procurement constraints, the Commission on Intelligence report of 1 March 1996 has defined such access as "critical", and recommended that dramatically improved analyst access to open sources be a top priority for the Director of Central Intelligence and a top priority for funding. This orientation discusses electronic access, the identification and acquisition of "grey literature", the identification and exploitation of international experts, and several examples of world-class international open source capabilities including Jane's Information Group and SPOT Image Corporation.

Chapter 4, THE INTERNET AS A TOOL FOR ALL-SOURCE ANALYSIS, presents a very broad overview of the global capability known as "The Internet" or "the Net". The Internet is a global communications medium that permits extraordinary flexibility in communicating with a wide variety of people from all walks of life, in receiving free information from many sources (some of dubious authenticity), and in obtaining access to distributed databases, many multi-media in nature, all over the world. This chapter will discuss in general terms the utility of the Internet to the all-source analyst, with special attention to the use of electronic mail, newsgroups, lists, and conferencing systems. It also discusses some of the dangers of the Internet, including the problems of "noise" and "flame wars", as well as the almost total lack of privacy and discretion. The last half of the chapter will focus on the most productive element of the Internet, the World Wide Web, and will provide five practical examples of how to exploit the Internet in support of the all-source analysis endeavor.

Chapter 5, OPEN SOURCES AND MILITARY CAPABILITIES, focuses on the practical application of open sources to military intelligence analysis requirements. The chapter begins by introducing a model for integrated all-source analysis which illustrates the critical importance of geographic and civil factors in evaluating the threat at each of the levels of analysis. While open sources are useful in conducting research and developing intelligence estimates about military capabilities in isolation, open sources are most useful to the military intelligence analyst when used to develop a broader analytical model. The general utility of open sources for military intelligence analysis, and the specific utility of open sources at the strategic, operational, tactical, and technical levels of analysis will be discussed. Next the chapter examines specific private sector capabilities for collecting and processing open source information. Commercial imagery, private sector order of battle information, and networks of experts available for consultation will be reviewed in general terms. Finally this chapter introduces the student to the Expeditionary Factors study developed by the Marine Corps Intelligence Activity, and used for this handbook because it is the only current and authoritative intelligence analysis product which relies exclusively on open sources, is unclassified in its final form, and covers a broad range of mission area factors for eighty countries specifically chosen because of the likelihood that a Marine Air Ground Task Force will be engaged in non-combatant or combatant missions in the countries

Chapter 6, OPEN SOURCES AND OPERATIONAL SECURITY--THE DARK SIDE, documents the premise that everything needed for the planning and execution of criminal or terrorist activity can be found in open sources. Indeed, an entire industry exists which is devoted to the publication of such material. In addition, equipment designed for one purpose and legally available can be used in terrorist or criminal activity. From both a military and a law enforcement point of view, it is critical to understand that even our most poorly-funded and least organized opponents can gain access to relatively sophisticated intelligence collection tools as well as tools of destruction.

Chapter 7, CONCLUSION: COLLECTING AND PROCESSING OPEN SOURCE, wraps up the handbook by providing information about three official U.S. government channels for obtaining open source intelligence: the Community Open Source Program Office and its global Open Source Information System; the Defense Intelligence Agency Open Source Program and the (planned) Defense Intelligence Agency Open Source Intelligence Center; and--especially important for Marines--the Marine Corps Intelligence Activity and the Expeditionary Factors Study. The Chapter concludes with a brief discussion of the usefulness of the Marine Corps Reserve as a source of existing and new open source exploitation experts, and some recommendations on additional open source training opportunities.

The APPENDICES provide both additional background information, and explicit references and points of contact which can be used to acquire open source intelligence in support of the commander and the staff. Appendix A, a White Paper on "Open Source Intelligence: What Is It? Why Is It Important to the Military?" was commissioned by the French Ministry of Defense and used (in translation) to begin the process of creating a French open source intelligence capability. Appendix B, consisting of both talking points and a formal paper on "Private Enterprise Intelligence: Its Potential Contribution to National Security" was developed as an invited paper for the annual open conference on Canadian intelligence. Included in Appendix B are a number of direct points of contact and key references useful in starting an open source intelligence program. Appendix C, a White Paper on "ACCESS: Theory and Practice of Intelligence in the Age of Information", was also commissioned by the French, and represents a somewhat abstract but still useful discussion of open source intelligence as a supporting discipline. Appendix D is a Concise Directory of Selected International Open Sources & Services which was prepared for the Defense Intelligence Agency, and remains both current and useful. Appendix E is a series of papers prepared for the Defense Intelligence Agency and serving as primers on exploiting the Internet, with over 100 pertinent intelligence-oriented sites and lists being identified in detail. Appendix F is a combination of a model (the original Expeditionary Environment Research & Analysis Framework & Model 1990) and strategic generalizations from the first Marine Corps Intelligence Activity study, *Overview of Planning and Programming Factors for Expeditionary Operations in the Third World*. Appendix G provides key references documenting what is available to terrorists and criminals which should be of concern to the military professional from an operations security viewpoint. Finally, Appendix H provides a list of the 80 countries examined in the current MCLA study, *Expeditionary Force Mission Factor Intelligence Analysis Requirements Study* dated 15 September 1994.

## Chapter 1

### OVERVIEW OF OPEN SOURCES & SERVICES

#### 1001. Purpose of the Chapter

The purpose of this chapter is to present a broad overview of open sources and services which are important to the all-source intelligence analyst.

Included in this chapter will be a definition of open source and a distinction between data, information, and intelligence; a brief discussion of the history of open source intelligence as a sub-discipline of the all-source intelligence process; a review of why open sources are important to military intelligence; examples of open sources and services which are not now commonly integrated into all-source analysis; and a discussion of open source exploitation within DIA (Defense Intelligence Agency) and in a number of allied intelligence communities.

This chapter concludes with a discussion of the changing role of the analyst; and how each analyst can take specific steps to improve their personal exploitation of open sources in support of the all-source intelligence process.

Appendices A and B are provided for background information. This initial chapter serves as the introductory element of the handbook.

#### 1002. Definitions

It is important for the professional intelligence analyst to remember that the final intelligence product is supposed to represent a refined process which integrates requirements analysis (defining what the customer needs to know), collection management, source validation, analytical integration, and presentation.

For the purposes of this handbook, the following definitions are provided:

-- *Data* is the raw print, image, or signal. Data can be classified, as in a technical intelligence signal intercept, or unclassified, as in a report from the Foreign Broadcast Information Service (FBIS) on a public television report. Please note that open source data includes commercial imagery such as is available from SPOT Image Corporation.

-- *Information* is data that has been collated, processed, in order to produce a report that is of generic interest. Information can be multi-media, with integrated graphics and imagery, or simply a print report including interpretation of imagery.

-- *Intelligence* in this context is used to distinguish those products which tailor information in order to support a specific decision by a specific customer.

*Nowhere is it written that "intelligence" must be classified.* A good intelligence product can be based exclusively on open sources, or only on signals intercepts--it is of course likely that the best intelligence will be "all-source" in nature, integrating an open source foundation with unique value-added insights from classified sources.

The *official* definition of *open source information*, established in Director of Central Intelligence Directive 2/12 (effective 1 March 1994) is: "publicly available information (i.e. any member of the public could lawfully obtain the information by request or observation). as well as other unclassified information that has limited public distribution or access". The latter is referred to as "grey literature" and includes non-proprietary information from companies and other organizations.

### 1003. Brief History of U.S. OSINT

The Office of Strategic Services (OSS), when first formed, was intended to serve primarily as a coordinator of information, and was initially constructed around a Research and Analysis Branch which relied almost exclusively on open sources. In fact, when the OSS later had significant but scarce clandestine collection capabilities, they utilized *The New York Times* to prepare "secret" reports to satisfy many of their customers' requirements which did not merit the risk or expense of clandestine collection.<sup>1</sup>

Over time, and after the Central Intelligence Agency (CIA) was created by the National Security Act of 1947, the responsibility for open source collection became fragmented between the federal departments, such as the Departments of State, Defense, and Commerce; and selected elements of the CIA which specialized in open source collection. The two most important, still existing today as elements of the CIA, are the Foreign Broadcast Information Service (FBIS), and the National Collection Division (NCD). The former monitors foreign print and broadcast media; the latter works with private sector parties to obtain unclassified information. Today the Community Open Source Program Office (COSPO) coordinates open source investments across the entire U.S. intelligence community. Most other organizations including the Defense Intelligence Agency (DIA) utilize External Research & Analysis (ER&A) funds to contract for open source collection and analysis from the private sector--however, these funds have been severely reduced in the 1990's as fiscal cut-backs and the desire to keep U.S. government personnel on board have led to great reductions in contracting for external (i.e. open source) assistance.

---

<sup>1</sup> Mile Copeland, *Without Cloak or Dagger: The Truth About the New Espionage* (Simon & Schuster, 1974), pages 47-48. Testifying to Congress in 1947, Allen Dulles himself stated "...in time of peace the bulk of intelligence can be obtained through overt channels...these overt, normal, and aboveboard means would supply us with over 80 percent, I should estimate, of the information required for the guidance of our national policy." As quoted in Peter Grose, *Gentleman Spy* (Houghton Mifflin, 1994).

In recent years, the "*information explosion*", together with major political upheavals within formerly denied areas, have made a vast quantity of open source information available to the public and to the intelligence community. Latin American investigative reporting, processed by Department of Energy laboratories, has been used by the U.S. Southern Operations Command to support Drug Enforcement Administration (DEA) interdiction operations; open source information is playing a critical role in countering proliferation, and in understanding transnational crime and especially financial crime.

Today, within the intelligence community and within Congress, there are differing views on the degree to which the intelligence community should collect and exploit open sources. Most observers, however, agree that the U.S. Intelligence Community should *not* be the focal point for open source collection *per se*, but that it *should* maintain a core capability to exploit private sector capabilities and to integrate global all source information into the all-source collection and production process. In practical terms, this means that *intelligence consumers are expected to manage and fund their own open source collection and production endeavors.*

#### **1004. OSINT & All-Source Analysis**

Open Source Intelligence, or OSINT, is an important part of the all-source intelligence process which includes clandestine Human Intelligence (HUMINT), Imagery Intelligence (IMINT), and Signals Intelligence (SIGINT). There are other important sub-disciplines, such as Measurements and Signatures Intelligence (MASINT) which analysts must understand and integrate to produce the best-possible intelligence.

Dr. Joseph Nye, then (1994) Chairman of the National Intelligence Council, used the jig-saw puzzle analogy to explain the relationship between OSINT and the classified disciplines. He likened open sources to the outer pieces of the puzzle, without which you can neither begin nor complete the puzzle. Classified sources, however, were essential to fill in the hardest to understand middle of the puzzle, and to complete the picture.

Mr. Paul Wallner, a member of the DIA Senior Executive Service, and the first Open Source Coordinator for the Director of Central Intelligence, described OSINT as "the source of first resort". His original conception was later adapted by a private sector commentator into the more dramatic phrase, "do not send a spy where a schoolboy can go" > Both drive home the point that open sources should be used to the fullest possible extent before risking and expending the more precious classified capabilities.

Dr. Joseph Markowitz, the current Director of COSPO, in addition to publishing the *Community Open Source Strategic Plan* (February 1995), has studied the utility of open sources in relation to traditional and emerging target sets, and concluded that open sources offer their greatest value as gap-fillers and initial orientations against Tier 4 Countries. Tier 4 Countries are those Third World countries which have not rated coverage by scarce classified capabilities, but to which the military must often deploy.



*In brief, open sources are not a substitute for classified capabilities, but they can provide a valuable foundation and context for rapid orientation of the analyst and the consumer, and for the establishment of collection requirements which take full advantage of the unique access provided by classified sources. Analysts must be careful about relying exclusively on classified sources, especially against Tier 4 countries, because often the narrow range of classified sources may mislead the analyst into accepting a narrow interpretation of events.*

## 1005. Knowledge Terrain: The Information Continuum

The figure below illustrates the "information continuum" which comprises the knowledge terrain of the private sector within which each all-source analyst must learn to navigate if they are to make the most effective use of classified as well as open sources. Appendix B has more detail on private enterprise intelligence capabilities.

K-12	Libraries	Private Investigators Information Brokers	Government	Intelligence
<hr/>				
	Universities	Businesses	Media	Defense

*Schools and Universities* are a source of both labor (student as well as faculty), and data. Mercyhurst College, for instance, which has the only undergraduate degree in the USA focused on producing trained intelligence analysts, has its students using open sources to produce newsletters on narcotics and other topics of interest to law enforcement agencies. Universities across the country--and around the world--serve as "centers of excellence" in various areas of interest to intelligence community analysts. Knowing how to access and exploit such distributed capabilities can save the analyst time, save the community money, and improve support to the consumer. *Libraries* offer similar opportunities, including the Special Libraries maintained by major multinational corporations and international non-governmental organizations.

*Businesses* maintain a great deal of information, much of it unpublished but available for the asking, on both conditions in the countries in which they do business, as well as about key personalities. During the war in Southwest Asia, it was businesses which provided the most critical information about Iraqi command & control systems, including the detailed plans for his installed communications and computing infrastructure.

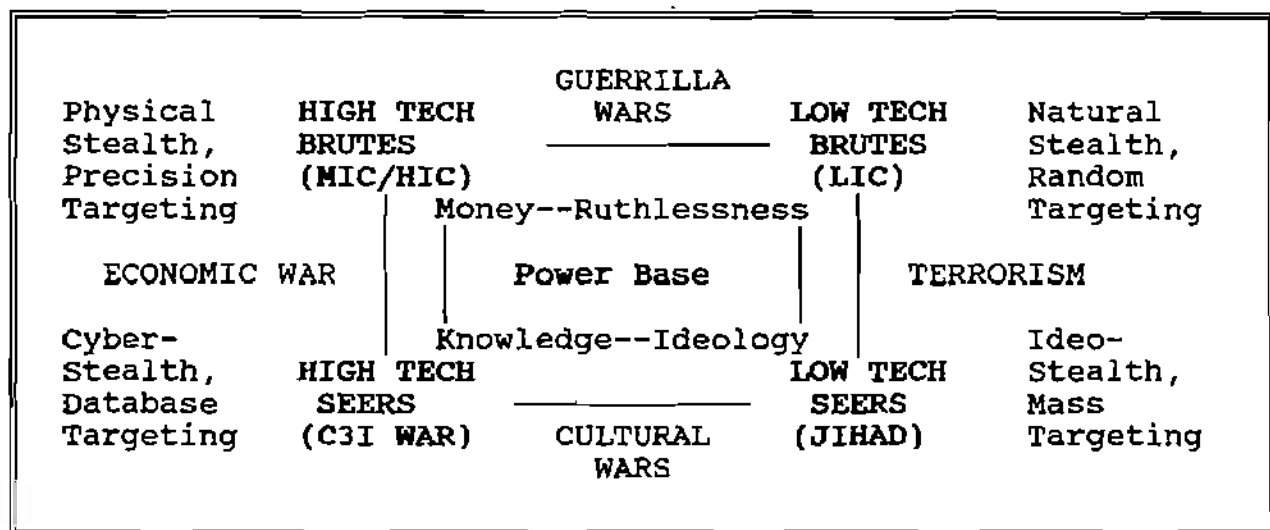
*Private Investigators and Information Brokers* spend their careers at someone else's expense developing expertise in certain areas and research methods. The *Burwell Directory of Information Brokers*, for instance, has specialists worldwide indexed by topic, country, and language fluency. They constitute a "ready reserve" for the intelligence analyst.

Few people realize that *media reporters* publish less than 10% of what they know, and are often happy to accommodate requests for information "on background". Although direct

contact by the analyst may not be appropriate, the analyst can use services such as LEXIS-NEXIS to identify experts in the media (e.g. the stringers covering Burundi or Somalia) and then task appropriate agencies with interviewing these experts along specific lines. Finally, analysts should catalogue their *counterparts* in other agencies and governments.

## 1006. OSINT and the Military I

The figure below illustrates the four warrior classes which confront both the military and law enforcement, and helps us understand that the intelligence challenges facing the military in the 21st Century require greater and distinct capabilities than those from the Cold War.



It is significant that our entire defense establishment, and our entire intelligence community, have been optimized over forty years to deal with just one of these warrior classes, the high-tech brute. The other three warrior classes represent significant intelligence challenges--the criminal, for instance, represents a "low-slow singleton" target which does not move high enough or fast enough, or emit enough of a signature, to be detectable by most of our space-borne early warning systems. The economic and computer warriors, the high-tech seers, represent both problems of jurisdiction, and problems of collection.

This training does not address policy, doctrine, or acquisition issues. The point of this chart is to both illustrate the challenges confronting intelligence analysts as they adjust to new targets; and also to make the point that open sources are--fortunately--both plentiful and pertinent when attempting to understand the three increasingly threatening warrior classes.

The information explosion has been a mixed blessing. Although a great deal of information about virtually every topic is available for purchase if not for free, the validity and utility of much of the information is questionable, and requires both heavy screening--

much of which cannot be done by machines--as well as translation and interpretation. All-source analysts today are trained to use classified tools and methods, and do not have optimal access to open source experts and databases.

Open source exploitation by DIA and the U.S. intelligence community is certain to improve, as this chapter concludes, because of the value of unclassified intelligence in support of unilateral information-based warfare, coalition operations, joint civilian-military operations, and support to law enforcement operations.

This chapter does not recommend that all-source analysts spend less time on classified sources and more time on open sources, but rather that they leverage private sector collection and production capabilities in order to optimize the collection management of classified capabilities.

## 1007. OSINT and the Military II

OSINT can be very important at each of the four levels of intelligence analysis. Appendix A provides additional discussion

*At the strategic level, analysts have found that a careful review of open sources, even from societies subject to censorship, can provide a sound understanding of political plans and intentions. Open sources are especially helpful in forecasting cultural turmoil and providing warning of revolution or upheaval. Also at the strategic level, open sources are very useful for developing the *encyclopedic generalizations* needed to develop theater capabilities for multiple contingencies. Finally, open sources are very helpful in orienting both troops and the public.*

*At the operational level, open sources can help force planning as well as the coordination of joint and coalition operations. It is open sources, for instance, which have established that the average temperature for expeditionary operations in the Third World is 80°, with high humidity. Since most aircraft are designed for "warm" days rather than "hot" days, this means that their range and lift are significantly reduced.*

*At the tactical level, open sources have proven valuable in obtaining commercial imagery and related products, including 1:50,000 combat charts with contour lines, for Third World areas for which the Defense Imagery Agency does not have digital data or ready maps.<sup>2</sup> Analysts requiring imagery and tactical maps to support a commander should not*

---

<sup>2</sup> Of 69 countries established in 1990 by the USMC as being "high probability" deployment areas, DMA had no data or maps for 22 of the countries; old maps for the ports and capital cities only of another 37; and very old maps for the remaining ten countries such as Cuba, North Korea, and Jamaica. *Overview of Planning and Programming Factors for Expeditionary Operations in the Third World* (MCCDC, March 1991).

hesitate to request commercial imagery. Commercial imagery products also include multi-spectral imagery sensitive to heat differences, and automated three-dimensional "fly-by" videos of approaches to airfields and landing areas.

*At the technical level, open sources are very important to developing information-based warfare capabilities and plans for attack; they are also useful in establishing realistic mobility estimates and weapons range and intervisibility (line of sight) needs.*

#### **1008. Militarily Useful OSINT: Two Examples**

Two examples are offered here of how useful OSINT can be, either as the foundation for a classified collection effort, or "in a pinch" when classified offerings are non-existent and unlikely to be quickly forthcoming. The first example, Somalia, was developed in support of a Marine Corps Wargame in which LtGen Zinni requested a post-mortem on his performance in Somalia. The individual invited to serve as the United Nations Commander for this wargame requested and received the following products via overnight mail:

- From Jane's Information Group, a one page map of Somalia clearly demarcating the nine clan areas; a one page order of battle for each clan including key artillery and mobility systems; and a compendium of one paragraph summaries with citations of every major article about Somalia published in any Jane's publication in the previous two years.

- From Oxford Analytica, twenty-two two-page summaries "suitable for a President or Prime Minister" covering U.S. foreign policy toward Somalia; UN operations in Somalia, and US operations in Somalia.

- From *The Economist* Intelligence Unit, a country study which, while shallow, had valuable insights regarding both the limitations and the fragility of the infrastructure.

Subsequently, in a second example, Burundi, the Commission on Intelligence requested and received, through overnight mail, products similar to the above from Jane's Information Group and Oxford Analytica, and in addition:

- From Eastview Publications, a list of all immediately available Soviet maps of Burundi, with their scale and price.

- From LEXIS-NEXIS, a listing of the top 25 journalists reporting on Burundi.

- From the Institute of Scientific Information, a listing of the top 10 academic knowledgeable about all aspects of Burundi.

Subsequently, it was determined that complete coverage of Burundi was available from SPOT Image Corporation, data already collected and stored, from which both 1:50,000 combat charts with contour lines, and landing point fly-by simulations could be created.

## 1009. Representative Open Sources I

Contract information for all of the references and organizations discussed in this handbook is provided in Appendix D. Most libraries will not have these references or access to these organizations--asking them to subscribe or develop support contracts is something anyone can do to improve your entire organization's access to key open sources.

**The British Library** specializes in monitoring international publications, and does especially well with respect to Africa and Asia, and conferences about both scientific & technical topics, and general topics including military matters. They are an especially good source now for examining the contents of conference *Proceedings*, and offer their products in CD-ROM.

**Oxford Analytica** is unique for having a global network of almost 1,000 overt human experts on-call to prepare concise forecasts and situation reports suitable "for Presidents, Prime Ministers, and you". They specialize in political-economic reporting.

A number of **directories** can help the analyst rapidly identify experts, many of whom are not likely to charge for quick informal inquiries.

- Specializing in **electronic** access is the book *Find It Fast: How to Uncover Expert Information on Any Subject*.

- For rapid identification of predominantly **academic experts**, the *Social Science Citation Index* and the *Science Citation Index* are unmatched--they are particularly useful in that they provide the expert's address, prior publications, and list of citations by others, establishing their peer recognition as authorities.

- **Government authorities** world-wide can be identified, with their full titles, addresses, and voice and fax numbers, through *Worldwide Government Directories*. Also available from the same organization is a biographic reference, *Profiles of World Government Leaders*.

- Finally, the best **private sector information brokers** world-wide, with complete contact information and indexes identifying their topical and language strengths, can be found through the *Burwell Directory of International Information Brokers*.

## 1010. Representative Open Sources II

**International research** sponsored by other governments, international non-governmental organizations, multinational corporations, and universities has been poorly documented in the past; now a new service, *ResearchBase*, is available which allows analysts to determine if there are projects underway which can be built upon rather than duplicated.

The Internet is--like the information explosion which it represents--a mixed blessing. Internet resources are in constant motion, and no search path can be duplicated from one day to the next. However, a number of entrepreneurs are beginning to offer useful guides. Among the three best are the *Clearinghouse for Subject-Oriented Internet Resources*; the *Guide to Network Resource Tools*; and *netguide*.

**Info-South** is an example of how universities can provide distributed database and media monitoring services to analysts. This service provides english-language translations of key Latin American newspapers, and also biographic profiles of Latin American leaders.

**Business community** information can be accessed through the Special Libraries Association, over 15,000 corporate librarians, through the publication *Inside Information: Profiles of Association Libraries and Information Centers*.

**Maps** are always very useful, both to the analyst developing the all-source product, and to the consumer, who often does not know where to go once DMA tells them no maps are available. The following two sources are helpful:

- **Eastview Publications** can rapidly identify and obtain maps of the Third World, generally down to the 1:250,000 level but sometimes better, which were created by the Soviet Union.

- **SPOT Image Corporation** has most of the world digitized at the 10 meter scale, and from this scale can create 1:50,000 combat charts with contour lines, targeting packages for precision munitions, and three-dimensional "fly-by" visualizations of landing site approaches.

**Unclassified photographs** can add value to intelligence reports; the archive of DoD photographs is now available through the National Technical Information Service (NTIS); a vast collection of international photographs is available from United Press International.

#### 1011. Representative Open Services 1

One of the most important changes in the open source world pertinent to the analyst is not the dramatic increase in the availability of raw data, but rather the significant improvement in the variety and capabilities of open services able to provide value-added collection, processing, and production.

Unlike direct acquisition requests for sources, these services generally have to be contracted for by the organization before they can be exploited; once a contract is established, however, individual analysts can then obtain direct support on demand.

**Academic Journal Monitoring** by Uncover Reveal or the Institute for Scientific Information allows analysts to receive tables of contents--via fax or email--for various

journals of interest, from which articles can be selected for acquisition.

**Commercial online searches** can be carried out directly by the providers, such as LEXIS-NEXIS or DIALOG, or through intermediaries such as NERAC. The former tend to be more efficient at exploiting their own databases, the latter has the advantage of charging a fixed price per year.

**Daily current awareness profiles** are a very good way of following the international media. The profiles generate daily lists of key articles, which can then be ordered if of interest. Besides LEXIS-NEXIS and DIALOG, the two most popular services are *Heads Up* from Individual, Inc., and *NewsEdge* from Desktop Data.

**Document Acquisition** world-wide is something private sector organizations do very well. Instead of burdening an Embassy with finding an obscure but essential document, organizations such as FIND/SVP can be relied upon.

**Environmental information**, of increasing importance to some intelligence consumers, depends heavily on commercial imagery as well as databases of environmental research. CIESIN (Consortium for International Earth Science Information Network) is among the leaders in this area.

**European Economic Research** is a specialty of Fuld & Company--specific research projects might be best conducted through a preliminary open source effort such a private sector company, followed by classified tasking.

## **1012. Representative Open Services II**

**Grey literature** refers to publicly available (non-proprietary) documents printed in very limited numbers and generally not available outside the country of publication. ACCESS International, and Eastview Publications, are among the best in this area.

**Infrastructure surveys**, including "ground truth" photography and surveying, can be done by some private sector organizations which employ former SAS (Special Air Service) personnel traveling discreetly under tourist or business cover. E2G, a British company, is one of the few that is openly available. In the US, BDM Federal specializes in remote infrastructure surveys, using legally obtained open sources.

**International investigations**, including economic surveys and technical acquisition projects, can be carried out by private firms such as Kroll Associates or Parvus-Jericho.

**Refugee debriefings** world-wide can be a gold-mine of raw intelligence. Organizations such as Rapport Research & Analysis, based in the UK, specialize in organizing teams of trained military interrogator-translators in any language, and then conducting debriefings in the major international cities where refugees are legally accessible.

**Third World economic analysis** can be contracted to such firms as SIS International, which had created a network of host-country business research organizations with special strengths in Asia and Africa.

**Telephone Surveys** are often a very low-cost means of creating new knowledge and obtaining a rapid sense of where a specific topic stands among leading authorities in the field. Telephone research is a special skill-set which includes a sound understanding of how professional associations around the world are organized and can be exploited. Risa Sacks Associates is one of the top US firms with this unique capability.

**Trade database creation** is a specialty of the Monterey Institute of International Studies, which is already very well known to the intelligence community for its use of graduate students fluent in Arabic, Russian, and other hard languages to create their proliferation database.

**Special comment:** in the open source world, niche providers outside the beltway are generally more capable, and cheaper, than large corporations based in Washington, D.C.

### 1013. Intelligence in the Age of Information

The two major differences between intelligence during the Cold War and intelligence today are as follows:

-- During the Cold War, the enemy was a well-known conventional power with nuclear capabilities, and the threat was relatively static over forty years. This led to the creation of an intelligence community optimized to do repetitive classified collection against a denied area, with a strong focus on major weapons systems with strong electronic and heat signatures. Today, as addressed by the earlier discussion of the four warrior classes, the threat is much more diverse, and consists of many smaller groups that are more difficult to identify, track, and analyze.

-- During the Cold War, the necessary information for intelligence analysis was generally not available through public sources; today much of what is needed to satisfy intelligence consumers is available from open sources, and the intelligence community is often in competition with open sources reaching the consumer directly.

Today, analysts must be responsive to their consumer's desires for intelligence reports that are short, fast, and often unclassified, for the latter can then be shared with Congressional staff and media as well as the public, and thereby help to influence policy change. *It is the consumer, not the analyst, who should make the decisions regarding preferred length, level of classification, and time permitted for report preparation.*

Classified information, which cannot be duplicated by open sources, represents a unique value-added capability--it will be most successful if it builds on open sources, rather



than competing with open sources or--worse--ignoring open sources and finding itself out of context and under-priced by "good enough" open source intelligence.

The most successful all-source analysts will develop methods of harnessing distributed experts and data in the open source world; do "just in time" analysis and production that supports specific decisions being faced by their consumers each day; stay close to the consumer to monitor and add value to the flood of open source reaching the consumer directly; and will master the art of integrating unclassified and classified products so as to give the consumer added power through more disseminable open source intelligence, and added confidence through the unique value-added insights that only classified all-source intelligence can provide.

#### **1014. Changing Role of the Analyst I**

The traditional all-source analyst has generally been focused in the task of monitoring and integrating classified intelligence (HUMINT, SIGINT, and IMINT) reaching their classified workstation, and has relied only to a very limited extent on the full range of open sources and services available through the private sector. At the same time, because of time, resource, and security constraints, the analyst has generally not interacted on a regular basis with either their private sector subject-matter counterparts, or their customers.

There is a growing belief that the role of the analyst must change in this decade, moving away from a relatively isolated emphasis on processing hard-copy and electronic intelligence into "products" that are then passed anonymously to a generic set of consumers through an impersonal broadcast, and toward a much more active--a much more interactive--role as a manager of people and resources.

Specifically, since no analyst can hope to master both the flood of classified and the flood of unclassified information, some envision the "reinvented" *analyst as a manager of a network of overt sources which serve as a foundation (not a substitute) for all-source collection and production*. Such a network, maintained by distributed centers of excellence in the private sector, at no expense to the government, could serve as a filter of subject-matter open sources, provide "tiger teams" for short periods to develop surge knowledge bases (e.g. Somalia, Rwanda), and help the analyst frame key questions which cannot be provided by open sources and must be tasked to classified capabilities.

#### **1015. Changing Role of the Analyst II**

At the same time, in order to manage and mobilize such a network of overt sources, the *analyst as a manager of resources* must emerge--an analyst that knows who the top experts are, and has the authority to hire them "on demand" for very specific and relatively inexpensive direct support tasks.

Although the intelligence community has received very fine support from a number of

major beltway corporations, these corporations have constituted an "outer ring" of institutionalized capabilities with the same limitations as the intelligence community itself.

The envisioned change in the role of the analyst brings with it the possibility of more direct analyst control over external research & analysis, with more analyst authority over day-to-day direct support contracts with individual experts rather than anonymous institutions.

The significant advantage of this approach is that the community pays only for what it uses, when it is used--this allows the analyst to take advantage of experts whose overhead--whose lifetime of acquired expertise--has been funded by someone else, someone other than the U.S. taxpayer.

#### **1016. Changing Role of the Analyst III**

Given the vast amounts of open sources that reach the consumer, there is increased interest in developing analysts able to serve as a *manager of consumer relations*, with three specific objectives:

- to win the consumers confidence on a day to day basis, and
- to ensure that the consumer is receiving appropriate decision support daily; and
- to monitor and exploit the open sources reaching the consumer.

It is very important for analysts to understand that consumers have and value their own open source connections, and they have and like to pay attention to their own departmental analysts.

The analyst, by developing a very close and constant relationship with their consumer, can not only gain access to the open sources that reach the consumer and do not reach the intelligence community--but can help the consumer avoid being taken in by open sources that might at first glance appear authoritative but which can--with the insights gained from all-source collection and analysis--be called into question.

#### **1017. Changing Role of the Analyst IV**

The professional intelligence analyst will always be different from scholars, journalists, and other expert commentators because only the professional intelligence analyst will have access to classified intelligence sources and classified intelligence tools.

The professional intelligence analyst that ignores open sources and relies exclusively on classified data for their raw input will not be competitive. In contrast to open sources, which represent the "information explosion" with all its pluses and minuses, the classified sources tend to be very finely focused and to produce narrow slices of information which

have to be melded and integrated. If you fail to use open sources to provide the context for analysis as well as the foundation for estimative intelligence, you will in all likelihood either miss the mark, or miss important tip-offs suggesting the need for classified tasking.

Open source information, therefore, should be seen as a pre-amble to fulfilling the analyst's ultimate responsibility as a *manager of classified capabilities* which lead to the production and delivery of an all-source product.

The role of open source information in the final product is important. At the Central Intelligence Agency, the general rule of thumb is that open source data comprises 40% of the final all-source intelligence product. Within the Defense Intelligence Agency, the general percentage, according to one graduate thesis survey, is 30%. In Canada, according to Mr. Ward Elcock, the director of the Canadian Security and Intelligence Service, open sources comprise 80% of the final all-source product.

What this means is that open sources are both a critical element in targeting classified capabilities, and also a critical element in explaining classified information in an all-source context.

Open sources are also very helpful when the analyst has classified sources which cannot be shared by the consumer with a specific audience (e.g. international organizations or the press) but which confirm the accuracy and utility of specific open source reports over others. Although the fact that the intelligence community lends its authority to specific open sources differentiates those sources at the time, this is sometimes the only way to provide intelligence in support of certain requirements.

#### **1018. Overt Human Networks: Some First Steps**

Most analysts know who their counterparts are at the other major intelligence agencies, and in the Joint Intelligence Centers (or, for law enforcement missions, the Regional Intelligence Centers). However, most analysts have not been afforded the time or given the incentive to identify and exploit their subject-matter counterparts in the private sector, and have perhaps also been concerned about the security implications of such contacts.

The analyst interested in evaluating the potential of the private sector to enhance their performance as an all-source analyst can take several steps in turn, with increasing management involvement, to achieve a unique status as a "hub" for both open and classified sources pertinent to their area of interest.

First, without engaging in any direct contacts of possible security concern, the analyst can inventory the private sector's capabilities in their area of interest, and rapidly establish a listing of key people--academics, journalists, business experts--who have something to contribute. At the same time, the analyst can inventory the availability of geographic information for their area of responsibility--as a former Director of the Marine Corps

Intelligence Center told the Council of Defense Intelligence Producers in 1992, "I don't care how much order of battle data you give me, if I cannot plot it on a (1:50,000) map. it is useless to me."

Jane's Information Group, which publishes both *Jane's Intelligence Review* and the *SENTINEL* series of *Country Reports*, also has an online database, and the capability to prepare special reports containing the 80% of the information they have about a country, but cannot publish for a variety of reasons including source protection.

Once the analyst has a good sense of who the top people are that might be of service as a personal network of overt sources, a few of these can be selected, and a specific plan proposed to management which seeks to fund individual familiarization meetings, possibly an exchange of unclassified data, and contingency arrangements for on-call support when required by a contingency.

Sponsorship of inter-agency subject-matter conferences, including an unclassified day with external experts, is a good way for the analyst to position themselves as focal points for voluntary information sharing.

#### **1019. OSINT Among Selected Allies**

In general, other intelligence communities are not any better off than the U.S. intelligence community with respect to open source exploitation. However, a number of them illustrate how improvements might be made in our own future endeavors.

Canada has gone on record publicly, stating that 80% of its all-source product comes from open sources; Canada is also a leader in doing unclassified strategic intelligence production which is receiving wide circulation and praise because it can be shared.

Israel has perfected the utilization of host-country information brokers, and exploitation of local laws such as the U.S. Freedom of Information Act, to obtain great quantities of information at almost no cost.

The United Kingdom, influenced by the open source movement within the U.S. intelligence community, has leaped ahead with the first public tender (Request for Comments) for an Open Source Information Center for the Ministry of Defence.

The United Kingdom Open Source Information Center is especially important because it could serve as a model for the United States of America, the other partners in the North Atlantic Treaty Organization, and the United Nation. An initiative to develop a center of expertise at the Joint Analysis Center (Molesworth) would be especially useful as a vehicle for linking United Kingdom and U.S. open source acquisition programs in the military arena.

## 1020. OSINT In Asia

In Asia there are several examples of strong approaches to open sources as a foundation for both national security and national competitiveness.

**Australia**, and specifically the Defence Intelligence Organization, has collected a significant amount of open source information on Papua New Guinea, the Spratley Islands, and other areas of interest to the U.S. Pacific Command, but they have no focal point for open source burden sharing.

**Japan** relies heavily on its private sector, notably the trading companies, for its open source collection, with a stated daily collection of 6,000 newsprint-size pages. Japan has also perfected "dissemination trees" in which each major organization collecting open sources from other countries--whether in the government or in the private sector--has roughly sixty other organizations to which copies are immediately routed.

**Singapore** relies primarily on open sources, and focuses heavily on economic intelligence. As a major banking center in its own right--and the likely base for those who choose to leave Hong Kong once it is turned over to the Republic of China, Singapore understands the value of providing its business community with a robust information environment. The National Computer Board (NCB) has representatives in every government department and is rapidly integrating all government databases. They will do the banks next--focusing on encyclopedic marketing information--and then elements of the private sector on a voluntary basis.

**Taiwan** has not been adequately studied, but it should be high on our list of countries to be observed because in Singapore, Taiwan is considered the "model" for open source collection.

## 1021. OSINT in Europe

**France** is actively orchestrating economic intelligence collection and education. In 1993, after the publication of the book *Friendly Spies*, and coincident with the privatization of a number of key French companies, the Prime Minister directed increased focus on the utility of open sources of intelligence. A conference was sponsored in October 1993 at which General Heinrich, then Director of Military Intelligence, and several other authorities including the leading U.S. advocate for open sources, made presentations to 300 leaders from across France on the subject of reinventing intelligence and using open sources. The government continues to play a strong role in organizing economic and information strategies, and in encouraging economic intelligence education.

**The Netherlands** has reorganized its collection to make open sources co-equal with technical and clandestine collection; uses a task force approach to analysis that begins with open sources; and optimizing its exploitation of the Internet by having specialists do

centralized discovery of Internet resources, while analysts do the decentralized exploitation of the resources once specifically identified.

**Sweden**, although small, has optimized its performance in science & technology by coordinating government, business, and academic collection of open sources through an informal committee called the Swedish Open Source Coordination Forum. The Swedish government is considering the "privatization" of the existing scientific & technical attache service, motivated largely by the need to decrease government spending. Swedish scientific & technical attaches have been aggressive about patrolling the Internet in search of both data and points of contact.

## **1022. OSINT Within DIA I**

The Program Manager for Open Source Intelligence within the Defense Intelligence Agency is Ms. Alice Cranor, whose contact information is provided here. She serves as the DIA representative to the Open Source Council, which is the advisory body formed to support the Community Open Source Program Office (COSPO). Each agency and service has a single representative to the Council. In addition to an agency-level focal point, every branch within DIA has an OSINT focal point.

The only survey to date of open source intelligence exploitation within DIA was completed in August 1995. "Open Source Intelligence: An Examination of Its Exploitation in the Defense Intelligence Community", by Major Robert Simmons, USA, is a Joint Military Intelligence College thesis which surveyed all analysts in DIA and its two production elements, the Armed Forces Medical Center and the Missile and Space Intelligence Center.

Maj Simmons' findings are shown here:

- Less than 30% input from open sources
- Such open sources as are used come through SAFE from FBIS
- Most analysts do not have Internet access
- Most analysts rarely discuss issues with external experts
- Most analysts are not aware of other open source resources
- Most analysts are generally satisfied with their level of access to open sources

Maj Simmons' concludes that the analytical components of DIA are generally "ill-prepared and ill-supported to make full use of any information outside of the small, restrictive and limited domain of classified intelligence sources. The cultural attitude at DIA generally reinforce(s) using classified information as the first and last stop in the analytical process and

open sources are used rarely to fill the gaps. The result is an intelligence product limited in its scope and overly expensive."

#### 1023. OSINT Within DIA II

Although the thesis results are negative with respect to existing DIA practices, and funding constraints do not appear to offer significant relief in terms of new initiatives to exploit open sources in support of military intelligence, there has been a significant increase within DIA of appreciation for the potential of open sources.

Maj Simmons' thesis concludes with these findings:

-- Tier 3 and 4 countries, where there is a very high probability of U.S. military involvement in contingencies, are not covered by established classified collection priorities.

Almost all of the countries of concern to the Marine Corps, as defined in the *Expeditionary Force Mission Factor Intelligence Analysis Requirements Study* (Marine Corps Intelligence Activity, 15 September 1994), are Tier 3 and 4 countries. In addition to a lack of encyclopedic intelligence, there also exist severe shortfalls in mapping, charting, & geodesy (MC&G) data needed to produce 1:50,000 combat charts for combined arms coordination and ground maneuver. Fortunately, commercial imagery, including 10-meter resolution imagery from SPOT Image Corporation, is capable of providing 1:50,000 maps with contour lines within hours or days--HOWEVER such commercial products still require assistance from classified capabilities orchestrated through the Defense Mapping Agency in order to integrate "ground truth" precision points needed to ensure the accuracy of the maps, as they are to be used for coordinating combined arms fires.<sup>3</sup>

#### 1024. OSINT Within DIA III

Continuing with the conclusions from Maj Simmons' thesis:

---

<sup>3</sup> Two major surveys have been done in recent years of MC&G short-falls in the Third World. The first was done by the Special Operations Command (J-2) in 1987-1988; and the second, focusing specifically on expeditionary contingencies, was done by the new Marine Corps Intelligence Center (now Activity). The Marine Corps Study, published as *Overview of Planning and Programming Factors for Expeditionary Operations in the Third World* (Marine Corps Combat Development Command, March 1990), found that of the 69 countries of concern to the Marine Corps, there were no combat charts at all for any portion of 22 of the countries; old combat charts for ports and capital cities only--not for maneuver areas--for another 37 countries; and very old combat charts for the remaining ten countries where higher priorities has permitted full coverage at one time--countries such as Cuba and North Korea.

-- OSINT is often the only resort in the early stages of a crisis, and critical in support of rapid-response planning for deployment--it should be noted that commercial imagery and 1:50,000 combat charts with contour lines from commercial imagery can be obtained within hours or days of demand.

-- Private sector publications such as those produced by Jane's Information Group often provide defense intelligence analysts with their first tip-offs on weapons modifications and sales.

-- Open sources serve as valuable tip-offs about national leaders' intentions, since actions are often justified in advance to their public through the press.

-- The majority of Third World terrorist information is obtained from FBIS and wire services (proliferation specialists say the same thing)

-- OSINT is essential when unclassified products are needed for coalition operations or briefings to uncleared Congressional members and staff.

What is the bottom line here: improved exploitation of OSINT as part of the all-source product is not going to be driven by top-down directives, but rather through bottom-up initiatives. Every analyst must understand the value of open sources, and the range of open sources and services available to support their subject-matter production requirements. Through a concerted effort by all analysts to request funding for access to open sources and services, defense intelligence will gradually be revitalized.

#### **1025. OSINT and the All-Source Product**

Concluding in this vein, recognizing that the analyst is the focal point for change in how we prepare the all-source product, this chapter suggests that each analyst must:

-- Strive to understand the information continuum and how private sector subject-matter experts and databases can provide direct support to the all-source process;

-- Develop a personal "map" of open source experts of possible value, including complete contact information. This is something which can be done without direct contact, as a pre-amble to securing management and security approvals for interaction.

-- Submit specific proposals to management for employing specific experts in specific ways to enhance the all-source intelligence product; and finally,

-- Work with security to establish comfortable ground rules for both planned and spontaneous contacts and unclassified information exchanges with external experts who will rarely have--or accept--security clearances.



The intelligence analyst is the critical linch-pin for reinventing the intelligence process and fully integrating open sources as a foundation for the all-source product. Those analysts that fully understand open sources, and develop proposals for exploiting open sources, will find themselves able to manage networks of overt open sources, able to justify and to manage modest resources to mobilize those open sources on demand; able to significantly improve their management of consumer relations and their exploitation of open sources reaching the consumer directly; and able to dramatically improve their management of classified capabilities, both in collection and production.

Open sources are not a substitute for classified sources--they are an essential and valuable foundation for making the most of our scarce classified capabilities.

## Chapter 2

### ACCESS: INTELLIGENCE IN THE AGE OF INFORMATION

#### 2001. Purpose of the Chapter

The purpose of this chapter is to present a more in-depth look at why open sources are critical to the all-source analysis endeavor, and how all-source analysts can optimize their exploitation of open source information.

Included in this overview will be: definitions distinguishing between data, information, and intelligence; discussions of how the art of intelligence is changing in the face of the "information explosion", the four kinds of information categories that an all-source analysts can consider accessing, and the three elements of information value; a discussion of the nine levels of open source information; an examination of possible collection management strategies which integrate open sources into the all-source collection management task and exploit windows of opportunity in which material is available in open sources just prior to being classified or censored; discussion of the four major consumer groups and their intelligence productions needs in relation to open sources; an examination of the four "warrior classes" and how open sources apply to intelligence analysis of each; discussion of the four types of overt human sources the analyst will encounter; an examination of how open source intelligence (OSINT) can help conserve scarce classified resources, and how a national information strategy can increase the amount of open source information available to the defense intelligence community; and concluding comments on optimizing OSINT in the all-source analysis process.

#### 2002. Definitions

For the purposes of this chapter, the following definitions are reviewed. This is a review of definitions provided in Chapter 1.

-- **Data** is the raw print, image, or signal. Data can be classified, as in a technical intelligence signal intercept, or unclassified, as in a report from the Foreign Broadcast Information Service (FBIS) on a public television report. Please note that open source data includes commercial imagery such as is available from SPOT Image Corporation, and from which 1:50,000 combat charts with contour lines can be quickly constructed.

-- **Information** is data that has been collated, processed, in order to produce a report that is of generic interest. Information can be multi-media, with integrated graphics and imagery, or simply a print report including interpretation of imagery.

-- **Intelligence** in this context is used to distinguish those products which tailor information in order to support a specific decision by a specific customer.

These definitions are important because the analyst will often deal with consumers and with questions where the best answer is an unclassified answer. The all-source analyst must avoid falling victim to the concept that only a classified answer has authority. The fact that the all-source analyst has access to classified information is what lends a special credibility to their selection of an open source and their provision to the consumer of an unclassified answer.

Intelligence consumers have important political and public responsibilities which frequently require candid discussions of "the threat" or "the situation" with individuals who are not authorized access to classified information. To the extent that the all-source analyst can provide the consumer with credible unclassified intelligence, the analyst will be facilitating the intelligence consumer's policy tasks.

### **2003. New "Rules of the Game"**

As the defense intelligence community moves away from focusing almost exclusively on the former Soviet Union and "denied area" intelligence, the all-source analyst is faced with requirements from new consumers, about threats and situations in the past which previously did not warrant all-source collection and production. Examples of such old but now more important intelligence problems include proliferation, terrorism, transnational crime, environmental threats, and economic intelligence.

Here are four new "rules of the game":

-- The National Foreign Intelligence Board has stated for the record that open sources comprise 40% of the all-source product, at a cost of less than 1% of the National Foreign Intelligence Program. For some intelligence problems, such as proliferation, and for some allied intelligence services such as the Canadian Security and Intelligence Service, open sources comprise 80% of the all-source product

-- The private sector has most of the real experts for those problems which are not traditional intelligence concerns. The Vice President has spoken about the need to "harness the distributed intelligence of the Nation". The all-source analyst needs to identify and exploit experts in the private sector and experts in allied governments.

-- Although electronic sources are fashionable, and most defense intelligence analysts rely almost exclusively on open sources collected by the Foreign Broadcast Information Service and delivered to their desktop workstation by the Secure Analysts File Environment (SAFE), in fact most open sources are in hard-copy, in a foreign language, and not available on the library shelves. Analysts must consciously define their open source requirements and set in motion the process to acquire the necessary open source material.

-- Analysts can no longer afford to do "just in case" collection and production. The demands on analysts are so extensive--almost overwhelming--that only a "just in time"

approach will permit them to satisfy consumers. This is especially true because information changes so quickly, that old archived information is usually overtaken by events. Analysts will do better going out to distributed databases at the last possible minute, and then integrating recent classified collection into their all-source product.

#### **2004. Four Information Categories**

The all-source analyst should understand that there are four information categories, and the relative cost and degree of difficulty for exploiting each category.

-- Open Source Information is legally and ethically available, at a low cost. The analyst that fully exploits open source information to establish a foundation for their all-source product can generally improve their understanding of the problem and its context at a low cost, and can often reduce requirements for classified collection.

-- Open Proprietary Information, can be legally and ethically obtained, but require a moderate cost to commission reverse engineering studies to extract the information from the product. This is a good alternative to riskier and higher cost espionage intended to steal the information from within the target organization. Examples: buying a French missile to study the missile guidance software and hardware; buying Russian imagery to calculate their overhead technical capabilities.

-- Closed Proprietary Information is only available from within the secure areas of the target organization, and requires espionage, at high cost, to obtain. Some intelligence services use private sector investigative agencies to obtain such information, under the guise of industrial espionage--a form of false flag operation. Examples: stealing source code for major computer applications; stealing designs for delicate machinery used to create scientific & technical instruments.

-- Classified information, collected by spies and satellites, is very expensive, and in the cast of Human Intelligence (HUMINT), often very risky. It does, however, have a very special value to the all-source analyst as its accuracy and reliability is high--this is especially the case with Signals Intelligence (SIGINT) products.

As analysts are thinking about an intelligence problem, they can benefit by drawing four circles around the problem definition. The outer circle, the largest, is the open source information domain. The analyst can annotate what open sources might offer insights to the problem. The next two circles moving inwards are open proprietary information and closed proprietary information. Finally, the smallest circle, classified information, can be annotated to show what precise and specific collection could help the analyst complete the intelligence puzzle. Using this method will help optimize the contribution of low-cost open sources while focusing demands on classified capabilities.

## 2005. Information Value

Here we want to consider the three elements which--taken together--comprise the value of information. Each is important because each can help the all-source analyst think about their collection management and production processes.

The raw content, a specific document, is often easy to obtain once it has been identified, but not so easy to identify. Any analyst who has ordered a commercial online search and received a listing of thousands of documents, with no means of sorting through them to determine relevance to the problem, will understand how difficult it can be to identify exactly the right document. Resources are scarce, and it is not cost effective to collect all possible documents and then review all personally. Analysts need to work closely with librarians and other open source collectors to refine the inquiry as much as possible. *Often, the best way of refining the inquiry is to consult a private sector expert--such as a defense industry expert--who is fully familiar with available content.*

The context within which specific content can and should be evaluated is often overlooked. For lack of both background and time, the analyst may not realize that specific cultural or political conditions give the content a meaning different from that which it might have in a U.S. context. *Again, consultation with a private sector expert--perhaps including a reputable journalist or a businessman resident in the area of interest--is often the best means of rapidly coming up to speed on context.*

Finally, we have timeliness. Analysts need to be sensitive to the fact that Foreign Broadcast Information Service reporting, while it contains value-added commentary, often arrives two to three weeks after it has been published. Internet news sources and commercial online services are more timely. "Near real time" media monitoring may not always be necessary, but analysts should consciously evaluate the timeliness with which they are receiving open source (and classified) information, and take steps to improve timeliness when it is important to the accuracy and relevance of their all-source intelligence production for the intelligence consumer.

## 2006. Open Sources

Here we briefly review nine levels of open source information. Future chapters in this course provide more detailed examination of sources such as the Internet.

The Internet is largely "free" once access is obtained, but analysts have to remember that "you get what you pay for". The reliability of Internet sources varies widely, and exploration of the Internet is very labor intensive, and can be misleading. For instance, analysts accessing the Internet through America Online or Compuserve need to know that they are seeing only those Internet sites pre-approved by their service provider.

Commercial online services are very useful, but represent the tip of the knowledge

iceberg. It is also critical for analysts to understand that commercial online services have different kinds of access and are not equivalent to one another. A CIA study found that of all the journals of interest to their analysts, one fifth were accessible through LEXIS-NEXIS (generally trade publications), one fifth through DIALOG (generally academic publications), one fifth through other online services (such as specialty scientific & technical publications), and *two fifths were not online* (such as Third World publications). Therefore, a collection strategy which mixes and integrates the different online services with hard-copy document acquisition is most likely to be successful.

Limited access electronic databases, such as are maintained by universities, industrial associations, or businesses, can over time be identified, and access gained through formal or informal contact. *Here again, overt human contacts are your best means of identifying pertinent databases that are not in the public domain but are accessible.*

Published literature and "grey literature " (limited edition publications) are the more commonly recognized mainstay of the open source world. *Do not overlook foreign language materials.* The *Burwell Directory of Information Brokers* will help the analyst identify professional searchers who speak a foreign language and are familiar with specific topics such as aerospace or nuclear proliferation.

Speeches and briefings are often overlooked as critical sources of "tip-off" on changes in policies and capabilities. In addition to LEXIS-NEXIS searches for media reports on such speeches, organizations such as The British Library carry conference *Proceedings*. Finally, direct interviews and sponsored external research complete the list.

## **2007. Collection Investment Strategies**

Realistically, the analyst is largely dependent on classified information that reaches their desktop workstation or their desk in hard-copy, and on such open source information that reaches them through SAFE. The analyst is also constrained by security and procurement processes that limit their ability to directly access external open sources including overt human experts.

Over time, we can expect progress in developing more direct access options for the analyst. In the interim, analysts can engage in several collection investment strategies where they allocate their time as a means of optimizing open source contributions to the all-source product.

First, analysts--in their role as collection managers--should pay heed to the words of Mr. Paul Wallner, the first Open Source Coordinator (and a member of the DIA senior executive service), who says that "open source should be the source of first resort". By focusing first on what is available through open sources, analysts will more quickly come up to speed on both content and context.

Second, analysts--in their role as resource managers--must recognize that it takes time to develop new forms of access, and that when they identify promising open sources which can contribute to the all-source intelligence production process, they should document their findings and make a business case for allocating funds to maintain access to such sources. Generally such resource planning must occur a year in advance of funds being obligated.

One investment strategy--initially addressing only how an analyst spends their time but ultimately suggesting how dollars might be allocated--would have the analyst spend twenty percent of their time identifying and analyzing open source information. It is important to note that because of the broadness of the open source environment, and the facility with which open sources can be exploited, a 20% investment of time or dollars yields dividends in excess of the investment, on the order of 50% or better of the contribution to the all-source product.

OSINT is well-suited to be the foundation for classified collection management through its provision of encyclopedic and contextual knowledge. However, classified sources must be used, and the analyst must create an integrated all-source product.

## **2008. Windows of Opportunity**

One of the interesting realities about scientific & technical intelligence which has been noticed by expert analysts over time is that often, critical information is published in open sources for a time before it is suddenly classified.

"Secrecy" is in reality an administrative classification of information. Analysts should be alert to precedent knowledge as a foundation for targeting classified capabilities against programs that have suddenly become classified. Censorship is in fact an excellent "tip-off" that a body of knowledge is now being exploited for military purposes.

Pre-publication opportunities for collecting knowledge directly from overt human sources are especially valuable, since "secrecy" tends to be imposed on written information rather than inherent knowledge. If an analyst cannot obtain approval for direct access to foreign scientists and observers, the analyst might consider developing an external research contract with key academics whose foreign travel and attendance at conferences can be funded. There will be significant regulatory guidance on what is permitted, and close coordination with established HUMINT agencies will be required, but the analyst can serve as a catalyst for targeting specific kinds of knowledge before it is published.

Pre-recognition of emerging knowledge areas is also a worthwhile analytical focus. Using citation analysis and bibliometric studies from such unique sources as the Institute for Scientific Information is a very good means of rapidly identifying clusters of knowledge experts and new trends in their relationships to one another. Bio-technology, for instance, could be anticipated by an analyst observing increased cross citations between biologists and computer scientists.

In the final analysis, *there is no substitute for peer contact*. Analysts must strive to identify, get to know, and interact professionally with their counterparts in the private sector. For these individuals are funded full-time by their institutions to follow the topic the analyst is interested in, and can often provide short-cuts and direct access to information that would otherwise take weeks or months to identify and exploit.

## 2009. Collection Management

There are a number of influences on how classified collection capabilities are actually managed, and analysts need to be aware of the relative priorities and the inevitable gaps in coverage.

Tier One and Tier Two targets (e.g. Russia, China, Germany) will generally receive solid coverage but occasionally require emphasis or follow-up. It is important to note that just because a target is receiving a Tier One or Tier Two priority, this does not mean that classified sources are providing comprehensive coverage. Open sources can provide invaluable additional information including contextual knowledge.

Tier Three and Tier Four targets (e.g. Somalia, Burundi, Haiti) will generally not receive in-depth coverage, and the analyst will have to be very specific about their requirements. It is possible to request a temporary increase in priority for an important "gap" in knowledge about the target. Open sources can be especially helpful in providing "tip-off" information and contextual information which will help the analyst make a case for a temporary increase in priority against a specific aspect of the target.

"Needs-driven" intelligence production, which is to say production that responds to direct requests from the intelligence consumer, is under scrutiny from Congressional staff because they are presuming that such requests are being communicated outside the existing priorities management system. Analysts need to exercise care and have the support of their managers when fulfilling "opportunity analysis" requests. Here, however, open sources will often provide a cheap and quick means of giving the consumer "good enough" intelligence without tasking classified capabilities.

Traditionally, consumers talk to analysts, analysts talk to collectors, and collectors talk to or examine sources. This is the "linear" paradigm for collection management. Increasingly, as open sources become more useful to intelligence consumers, and security obstacles are gradually eliminated, a new paradigm is utilized, the "diamond paradigm". This means that consumers, analysts, collectors, and open sources can and should talk directly to one another, as a means of improving communications, avoiding misunderstandings, and getting "real time" answers from the source to the consumer.

The bottom line for analysts in the open source world: the more overt human sources you can develop in your field of expertise, the more ACCESS you will have to useful OSINT.



## **2010. Four Major Consumer Groups**

In developing their research plans and thinking about how to craft their all-source products, analysts can benefit from an understanding of the four major intelligence consumer groups, each of which has a different "level of analysis" interest.

At the strategic level, departmental consumers are concerned with strategic generalizations and with the plans & intentions of their counterpart leaders across the board, in all regions. For example, if an analyst were to examine all of the countries where the contingency employment of U.S. troops is likely in the next few years, they might find that all of the countries less one or two are characterized by very high temperatures and humidity. This is an important strategic generalization because it impacts on aviation capabilities by reducing the amount of lift and the range of aircraft. Departmental planners can thus benefit from understanding that their "average" aviation capability in most contingencies will be less is assumed by doctrine.

At the regional level, theater commanders and their staff need regional generalizations and detailed mobility studies. For example, very few operational staffs will focus on port clearances (the deepest ship draft), the location of the five fathom line (critical to naval gunfire support), or the distance of the Embassy from the five fathom line (which determines if CH-46's can get there and back without Forward Area Refueling Points). Analysts able to draw out such generalizations will be able to provide a regional intelligence model that is very useful. Most of this information is available from open sources.

At the tactical level, mission area specifics and demographic and cultural studies are helpful. Most of this information is available from open sources, and in the case of demographic and cultural information, is often available only from open sources.

At the technical level, in addition to mission area specifics, it is helpful to develop realistic assessments of the degree to which both friendly and enemy capabilities are supportable by their respective logistics and intelligence capabilities.

There is no "schoolbook" solution for how to shape an intelligence analysis product in relation to the likely consumer, but if analysts are sensitive to the "level of analysis" that their consumer requires, they can provide intelligence products which are more meaningful and which reduce the burden on the consumer to sift through products.

## **2011. Intelligence Production**

Continuing our discussion of the "level of analysis", here we can see that open sources have a great deal to contribute to the all-source product at each level.

At the strategic level, much of the information about military sustainability, including the availability of fuel, water, and rations, can be obtained through analysis of open sources.

The analyst that understands history and geography can exploit open sources to establish a good sense of how geographic location and civil allies might influence plans and intentions.

At the operational level, open sources are not only vital, but often more pertinent than classified sources when studying military availability, geographic resources, and civil instability. Jane's Information Group is regularly credited by analysts with providing "tip-offs" on new weapons acquisitions. A sound understanding of geographic resources can help analysts interpret various scenarios, some of which may not be supportable (or may be driven by) a lack of resources such as oil. Civil instability is especially understandable through open sources. One Department of State analyst, studying the possibilities for instability in Iran in the event of the leader's death, found that clandestine sources tended to reflect the biases of the sources, all former officers under the Shah, and that local newspapers, despite censorship, were provided the most accurate sense of the situation. *Foreign language skill is essential to derive the fullest possible benefit from open sources.*

At the tactical level, while military reliability (troop training, equipment maintenance) is best established through classified sources, open sources offer a great deal. Here it is important to understand that organizations like Jane's Information Group have a great deal of information about military reliability that they do not publish, but which is available on demand. Geographic terrain, particularly for the bulk of the Third World for which the Defense Mapping Agency does not have data, can be studied through commercial imagery. Very few people in Washington realize that 10 meter commercial imagery is adequate for the production of 1:50,000 combat charts with contour lines, as well as simulated three-dimensional fly-bys. SPOT Image Corporation can provide these products for anywhere on earth within 24-72 hours.

Finally, at the technical level, open sources are especially useful in evaluating the civil infrastructure, including the telecommunications, power, and financial networks.

## **2012. Target Categories**

Each area of operations is likely to have a mix of four different kinds of "warrior class" which must be studied. These distinctions are provided in order to help the analyst broaden their effort beyond standard order of battle information, and to emphasize the utility of open sources in understanding non-traditional capabilities.

The traditional opponent which the U.S. has prepared for is the "high-tech muscle" warrior, represented by most of the Western allies and such major powers as Russia and China. This also includes powers such as Iraq which have invested heavily in expensive and sophisticated mobility and weapons systems. Existing classified collection capabilities are best suited for studying this warrior class, as the military systems generally emit heat or have clearly recognizable electronic signatures.

The next most understood warrior class, the "low-tech muscle" warrior, is generally associated with low intensity conflict scenarios. This warrior class is very difficult to track using existing classified capabilities because it represents the "low slow singleton" problem. This class of warrior utilizes single human couriers, Cessnas, and unsophisticated means of communications which do not lend themselves to interception. Surprisingly, open sources turn out to be useful against this class of warrior. The best example of a "success story" is found in the Southern Operations Command, which worked with the Los Alamos National Laboratory to obtain, translate, and study Latin American newspaper articles about drug activities in Latin America. SOUTHCOM discovered that Latin American investigative journalists are very good and provided complex reporting on the relationships between drug cartel members, the supply routes, the arrival of precursor chemicals, and a wide variety of other useful information.

The least understood warrior class is the "low-tech brain" represented by Islamic fundamentalism, for example. This is a warrior class for which open sources are the only viable means of understanding its plans and intentions. However, the open source materials to be mastered are so voluminous, and almost always in a foreign language, so that this becomes a very labor-intensive activity. Against this kind of problem, overt human experts in the private sector often offer the shortest route to insights.

Finally, the "high-tech brain" warrior class, now very popular as we think about both information warfare and economic warfare...here open sources play a very important role. Examples include hackers, electronic bank robbers, and industrial spies.

### **2013. Types of Overt Human Sources**

The purpose of this chapter is not to over-generalize or to categorize all human sources into four groups, but rather to stimulate analyst consideration of what biases and accesses might be represented by any particular overt human source whose written or verbal work they are integrating into the all-source product. These generalizations are offered for discussion purposes only!

These categorizations are drawn from a French source with a strong background in clandestine intelligence, who has spoken publicly on open source intelligence methods.

"Ivory Tower" academics, irrespective of their cultural backgrounds, tend to quote one another and to focus on abstract aspects of a problem in isolation from political and economic realities.

"Band-Wagon" journalists, always following the latest story, have a tendency to write about whatever the latest trend is, whatever the latest "spin" is on a story.

"Mainstream" operators are bound by their institutional or political loyalties to cite the conventional wisdom.

"Up and coming" leaders are the best source for tip-offs on emerging trends and plans and intentions, because they are change agents and more likely to put forth innovative and controversial ideas.

In evaluating the range of open sources that can be collected and integrated into an all-source product, the analyst might wish to consider each open source document with respect to the above four categories, and then to search for open source materials from those categories that are not yet represented. In this fashion, a "collage" of opinion can be charted which is more likely to offer insights, and to provide a solid context for the integration of classified intercepts and other classified materials.

#### **2014. OSINT As A Resource Saver**

Apart from its value as "content", as part of the all-source solution, open sources offer significant savings when they are used to avoid waste and unnecessary tasking of classified intelligence capabilities. It is sensible to avoid sending a spy where a schoolchild can go. It is also sensible to understand that intelligence products which limit themselves to classified sources are likely to miss important contextual knowledge and perhaps suffer from serious misperceptions.

Open sources can be the foundation for establishing a more efficient and more focused classified collection management plan. Open sources can be a means of satisfying intelligence consumers with "good enough" answers that avoid tasking classified systems at all. Open sources can be supportive of classified collection targeting, by helping the analyst identify specific human, communications, and organizational targets so that classified capabilities can be "pin-pointed".

Mr. Keith Hall, Director of the Community Management Staff, coined the term "ASK-INT" when he was a member of the professional staff of the Senate Select Committee on Intelligence. Too often, he noted, classified capabilities were tasked to obtain information that could be had for the price of a telephone call. Naturally there will be times when the analyst does not wish to reveal interest in a topic, but there are means for asking open source questions through contracted private sector parties at a lower cost than would be incurred when assigning the question to classified capabilities.

In the signals intelligence arena, open sources have proven to be extraordinarily useful in monitoring conditions across entire nations and in specific areas of interest such as the political and economic arena. For example, analysts tracking regional newspaper stories and editorials can form very accurate impressions about stability and changes in political power. Open sources also provide very valuable information about telecommunications networks (for example, the exact location and nature of power plants, telephone switching stations, and satellite downlinks) which can be used to target classified capabilities.

In the imagery arena, commercial imagery is now available at 10 meters resolution from SPOT Image Corporation, and 2 meter resolution from the Russians. A variety of other commercial imagery providers are emerging, some offering 1 meter resolution imagery capabilities. Low cost commercial imagery, and maps, are a very important resource saver.

## **2015. National Information Strategy**

The national and defense intelligence communities are part of a much larger information continuum, discussed in Chapter 001. One of the challenges facing our Nation as it enters the Age of Information is that of fully exploiting open sources, and ensuring that the broadest possible range of open sources are available to the national and defense intelligence analyst.

The Defense Information Infrastructure (DII), the National Information Infrastructure (NII), and the Global Information Infrastructure (GII) are part of an innovative and comprehensive effort by the current administration to develop increased connectivity across all sectors of the information continuum.

As the Vice President of the United States of America has noted on many occasions, the NII seeks to "harness the distributed intelligence of the Nation". What this really means to the professional intelligence analyst is that new means are being developed which will allow the analyst to access distributed centers of excellence where overt human experts and unclassified electronic databases are maintained. This is helpful to the intelligence community because it enables exploitation of expertise that has been funded by the private sector.

Still lacking for the intelligence analyst is an inventory of such centers of excellence as they apply to the needs of the various functional area specialists. In the interim, each analyst must attempt to identify such centers on their own, and to then work with the library and other collection channels to develop regular access.

An opportunity exists for analysts to take the initiative in developing international unclassified burden-sharing agreements with their counterparts in allied intelligence agencies. Australia has unclassified information on the South Pacific, France and Italy on Africa, and so on. Creative exchanges of unclassified information could be helpful.

Finally, it is important to stress that the existing electronic infrastructure for accessing open source information is not secure. Analysts need to recognize that Internet transactions can be monitored, that viruses are rampant outside the TEMPEST environment afforded by the intelligence community, and that there are many security hazards, both in terms of monitoring and in terms of destructive software, in the open source world. A national information strategy will begin the process of making it safe to work in cyberspace.

## 2016. Optimizing OSINT

The purpose of intelligence is to inform the policy-maker and the commander.

In developing their collection management and intelligence production plans, the analyst should consider the following paraphrase from the Navy Wing Commander who led the lead flight over Baghdad during the Gulf War:

*"If it is 80% accurate, on time, and I can share it, this is a lot more useful to me than a compendium of Top Secret CODEWORD information that is too much, too late, and needs a safe and three security officers to move it around the battlefield."*

Navy Wing Commander  
Technology Initiatives Wargame 1992  
Naval War College, Newport RI

In striving to satisfy an ever-growing demand for intelligence, about an always expanding range of topics, the analyst will have to adopt the traditional public administration principle of "satisficing", working to provide the intelligence consumer with "good enough" intelligence. Just as "better" is the enemy of "good enough", excessive reliance on classified capabilities which are already over-tasked, can be counter-productive to the task of informing the intelligence consumer.

In the chaos of the 21st century, the distributed centers of excellence in the private sector which collect and process open source information, are the analyst's first line of defense--as Mr. Paul Wallner has noted, "the source of first resort".

Ultimately the all-source analyst is responsible for thinking in context and ensuring that the policy-maker and the commander receive the best possible intelligence product. Open sources are not a substitute for classified sources--they are a contextual and encyclopedic foundation for thinking about the problem. Open sources are the means by which the all-source analyst extracts the greatest possible return from classified sources.

In the Age of Information, "intelligence" is defined less by whether it is classified or unclassified, and more by whether it is on time, on target, and useful to the consumer.

## **Chapter 3**

### **INTERNATIONAL OPEN SOURCES AND SERVICES**

#### **3001. Purpose of the Chapter**

The purpose of this chapter is to provide an orientation to international open sources and services which are available to the all-source analyst. Although much of the open source world is not yet easily accessible to analysts because of security and procurement constraints, the Commission on Intelligence report of 1 March 1996 has defined such access as "critical", and recommended that dramatically improved analyst access to open sources be a top priority for the Director of Central Intelligence and a top priority for funding.

This orientation will discuss electronic access, the identification and acquisition of "grey literature", the identification and exploitation of international experts, and several examples of world-class international open source capabilities including Jane's Information Group and SPOT Image Corporation.

Appendix D provides a concise directory (including complete contact information) for all international open sources & services discussed in this chapter. There are many, many more international sources available to the analyst which can be readily identified either through traditional library research, or through direct contact with international experts who can tell the analyst what sources they have found most useful for specific topics. The References are good starting points for additional direction.

#### **3002. American Online Services**

Most people unfamiliar with the world of open sources think of America Online and COMPU SERVE when they think of "online services".

In fact, "real" commercial online services, the kinds used by professional information brokers and specialists world-wide to do serious research, are completely different in nature and operation.

LEXIS-NEXIS and DIALOG are the two premier U.S. commercial online services. They each offer, for specific subscription and access fees, a wide range of electronic libraries. Access can be as cheap as \$20 for a quick search, or \$70-100 an hour for a complex search. It is best to work with an expert searcher to save money.

It is very important to understand that these two services are complementary and that searching one of them by themselves will not produce the best possible online search results. In the early 1990's a survey was conducted of all analysts in the Central Intelligence Agency, and each was asked to list journals of importance to them. The survey found that one fifth of the journals were available through LEXIS-NEXIS, one fifth through DIALOG, one fifth in

CD-ROM or electronic form, and two fifths were not available online.

American online services, although they have shown significant improvement in the past few years, are still primarily a source of English-language materials from the mainstream of the Western hemisphere, and specifically the United States and the United Kingdom.

America Online and COMPUSERVE are the equivalent of the corner drugstore when compared to the far more robust and extensive holdings of LEXIS-NEXIS and DIALOG "libraries". They do, however, offer very fine interfaces to the world of newsgroups as available on the Internet, and they also offer a number of organized conferences (such as the Military Forum in COMPUSERVE). Most people think of these services, available for around \$25 a month, as cheap, but in fact that is only the basic access cost--once the per hour online charges are added, those who spend a lot of time browsing can find themselves spending \$200 a month. Direct access to the Internet, including free NEWSNET services, is available for \$20 a month from numerous services such as UUNET, Capital Area Internet Services, and DIGEX.

### **3003. Foreign Online Services**

The world of foreign online services is more complex, and for the analyst concerned with international matters, often more rewarding. Unfortunately, these services are not routinely available to the U.S. intelligence analyst today. They are, with the increased emphasis on open sources brought about by the Commission on Intelligence, likely to be made available if requested by the analysts. Their fees are comparable to US services.

The Derwent World Patents Index (DWPI) is the most comprehensive database of inventions published worldwide. Every week more than 20,000 patent documents from 40 countries are processed into patent families, that is, groupings of patent documents from different countries covering the same invention. Each record has an English language abstract, is fully indexed, and is online. Selected technical drawings are included in the online holdings. Generally comprehensive coverage of all technology dates from 1974.

Questel/Orbit is an international online service specializing in patent, trademark, scientific, chemical, business, and news information. It was the first company world-wide to provide access to patent drawings online. Its holdings include materials from the European Patent Office, Japan Patent Information Organization, and the U.S. Patent Office. This service also focuses on international trademarks, and on scientific & technical research, breakthroughs, and products.

STN International, standing for (the Scientific and Technical Information Network) is an online search service providing direct access to over 190 scientific, technical, business, and patent databases. STN is operated jointly by the Japan Information Center of Science and Technology in Asia, by FIZ-Karlsruhe in Germany, and by CAS in North America.



GaleNet is the new online service from one of the most prominent and reliable publishers of international directories such as the *Encyclopedia of Associations*, the *Guide to Internet Databases*, the *Gale Directory of Databases*, and the *Research Centers and Services Directory*.

International Thomson Publishing does not offer its basic references online, but it does offer a free online search service which is useful, allowing simple searches by author, title, or other user-defined search criteria. Among the titles they publish are *Geographic Information Systems: A Guide to the Technology* (1991).

### **3004. Information Brokers**

What is an information broker? The short answer is: the information broker is and can be an analyst's best friend. This is an individual who specializes in discovering, evaluating, and distilling information available from public sources, in order to answer a specific question from a customer. They generally charge between \$70 and \$120 an hour inclusive of search fees (they are expert at keeping the online cost down, but their offline expertise is valuable), plus between \$15 and \$60 for individual document delivery. Generally online searches identify the existence of specific documents, which must then be located in a library, copied, and faxed to the buyer.

Perhaps most importantly to the analyst, information brokers tend to specialize in specific scientific and technical, or industrial areas, and so over time they build up an in-depth knowledge of open sources and methods which can be of invaluable assistance to the analyst working a short-fused problem set. This is important: a good information broker can save the analysts days if not weeks of preliminary research.

The *Burwell World Directory of Information Brokers* is available in both hard and soft copy, and is indexed by subject matter as well as by foreign language expertise. Ordering information is provided in the hand-out.

Information brokers differ from all-source analysts in two important ways:

First, they specialize in discovering, evaluating, and distilling information for a client, but they do not conduct the kind of analysis and estimative forecasting that a typical intelligence community analyst is expected to perform; and

Second, they deal only with unclassified public sources which are legally and ethically available.

Having said that, there is much that analysts can learn from information brokers. Two books, for which complete ordering information is provided in Appendix D, are especially recommended:

Reva Basch, *Secrets of the Super Searchers: The Accumulated Wisdom of 23 of the World's Top Online Searchers*; and

Sue Rugge and Alfred Glossbrenner, *The Information Broker's Handbook*.

### **3005. Grey Literature**

A major obstacle to U.S. understanding of foreign events, foreign cultures, and foreign plans and intentions is the fact that most of what is published about these foreign targets is in a foreign language and generally published in limited editions which are not readily identifiable, translatable, and reportable by existing U.S. intelligence capabilities.

"Grey Literature" is a growing field of interest, as experts worldwide begin to focus on the importance of "niche" information. Because grey literature is not "mainstream" and is often not electronic, the challenge of identifying and obtaining just the right piece of information requires the employment of expert intermediaries.

Examples of grey literature include trade show information, conference proceedings, unpublished "pre-prints" or works in progress, local area telephone directories, university yearbooks, and mailing lists for specific industries or countries.

Information brokers remain one of the best paths to grey literature because these information brokers specialize in selected areas and by virtue of their constant focus, are aware of new publications as they emerge, and are also in contact with key people in foreign industries and governments who can help them obtain selected materials not on the public market but still legally available in limited numbers. The *Burwell World Directory of Information Brokers* is unique for having an index identifying individual brokers based on their foreign language, foreign database, and foreign residence knowledge.

Professional associations, including U.S. associations, are a very rich source of leads and often will provide original source materials at no cost. At a minimum, professional associations can help analysts quickly identify authoritative individuals in specific countries who can be approached with a question or request.

Finally, international experts who are not information brokers and may not be associated with any professional association, are key players in linking analysts to exactly the right information. Two means of identifying such experts will be discussed momentarily.

### **3006. Document Acquisition**

Before looking at international experts, it is useful to examine several services which specialize in document acquisition. The most prominent of these, with offices world-wide, is FIND/SVP, where SVP stands for the French-language phrase "if you please". FIND/SVP

has a major office in New York, and operates both a "quick find" service that will locate two or three relevant articles upon telephone request, and a more in-depth strategic research arm.

CISTI is the Canada Institute for Scientific and Technical Information; it provides world-wide scientific, technical, and medical information services, and also provides at no cost online, the CISTI Online Catalogue. One of the special features of CISTI is its collection of conference proceedings and serial reports.

Disclosure, Inc. has teamed up with American Business Information to provide access to high quality mailing lists and company financial and credit reports. Although publicly traded companies have the most information available, privately owned companies also have financial statements and credit reports, and primary research through industry experts (such as the editors of trade newsletters) can uncover more information. They also have a world-wide presence and can respond to document acquisition requests in their area of expertise.

Genuine Article is the document delivery service offered by the Institute of Scientific Information, which is unique for having a global citation analysis database in both science and social science. Citation analysis is a uniquely valuable analytical tool. The references tell the analyst who has cited or is cited by any major article in academic, scientific & technical, and international business literature. This allows the analyst to determine several things: taking a known relevant work, to determine who has done the latest work in this area, identifying them through their citation of the relevant work; taking a known author, rapidly establish the author's peer standing and influence through citations by others; or taking a specific area of inquiry, quickly cluster the different expert groups through their citations of one another.

Uncover Reveal is an online periodical article delivery service and a current awareness alerting service. It indexes nearly 17,000 English language periodicals in its database. There is no charge for searching the database; articles ordered can be delivered by fax, often within one hour.

### **3007. International Experts I**

Analysts forced to rely on "umbrella" support contracts with a few specific intelligence industrial base companies will often find that these companies are simply one bureaucracy removed from the government, and do not have the flexible access to international experts that is needed.

One solution for analysts is to use in-house access to commercial online services such as LEXIS-NEXIS and DIALOG, to identify international experts.

In two different exercises, one on Somalia for the Marine Corps and one on Burundi for the Commission on Intelligence, LEXIS-NEXIS proved superb at identifying the top twenty-five journalists whose by-lines suggested they were expert on the country on which

they were reporting. Such individuals could be easily contacted for background information and insights on emerging trends. It is worth noting that journalists publish less than ten percent of what they know, and often have an understanding of personalities and motivations that they can share off-line but could never publish.

At the same time, using commercial online sources to search for quoted experts is a fast means of locating key individuals whose expertise has already been evaluated and is now relied on by journalists. Their knowledge will be different from that of the journalists.

Finally, since both LEXIS-NEXIS and DIALOG carry the transcripts of Cable News Network and other major international broadcast media such as the British Broadcasting Network, it is also possible to identify the "world-class" experts that are routinely called upon to comment on air.

### **3008. International Experts II**

A second and deeper means of identifying experts is to work through the capabilities provided by the Institute of Scientific Information, and its unique proprietary publications and databases.

Both the *Social Science Citation Index* and the *Science Citation Index* were created to perform a unique service which is not available from any other source: they identify who has cited whom up to date (generally up to within three months). This allows an analyst to take a known work that is directly pertinent, and by examining who has quoted that work, to quickly identify those who are publishing in the field today.

Perhaps even more importantly, the Institute of Scientific Information is able to perform bibliometric analysis on all of this data, and cluster papers according to their influence. "Bibliometric" refers to the study of citation patterns and their meaning, rather than to content analysis. In effect, individual papers can be evaluated based on the degree to which they were considered relevant by others, and at the same time the relationships between different authors and schools of knowledge can be plotted using clustering techniques.

Finally, complete addresses and contact information are available for each author, enabling an analyst to quickly establish direct contact with an individual whose publications and peer citation establishes them as a high-value subject matter expert.

### **3009. International Directories**

There are many international directories, but a few stand out. Ordering information for all of these are contained in Appendix D.

The *Encyclopedia of Associations* is a unique tool for it identifies key professionals in

every scientific and technical endeavor, and often permits direct contact with individuals who would otherwise be constrained by corporate non-disclosure terms.

The *Worldwide Directory of Government Officials*, updated frequently, is a comprehensive source for complete names, titles, telephone numbers, and even fax numbers for government officials from defense, intelligence, and all other government departments.

The *Research Centers Directory* and the *Directory of Publications and Broadcast Media* are examples of useful tools for getting in touch with key people.

A number of excellent references, all listed in the hand-out, are published by The Reference Press, Inc., and these include directories of key contacts in the various geographical regions of the world.

Finally, the International Supplement to The National Directory of Addresses and Telephone Numbers.

It merits comment that even without any directories at all, an analyst willing to use directory assistance, including international directory assistance, should, in the space of four telephone calls, be able to identify somebody with knowledge useful to the problem at hand. An example: an analyst interested in environmental conditions in an area not covered by any directory, could call directory assistance in that country, ask for any listing beginning with the word "environment" in the local language, and within four telephone calls probably identify someone who is moderately familiar with exactly the information desired.

The bottom line: if you are persistent, the telephone really can help you reach out and touch someone.

### 3010. Jane's Information Group

Jane's Information Group has long been a primary source for many military intelligence analysts. In his thesis on *Open Source Intelligence: An Examination of Its Exploitation in the Defense Intelligence Community*, then Major (now LtCol) Robert M. Simmons found that many analysts relied on Jane's for tip-offs about new weapons developments and technology transfers.

Among the more obvious benefits from Jane's Information Group are its widely admired publications, *International Defense Review*, *Jane's Intelligence Review*, and of course its entire series of handbooks on different weapons and mobility systems, now available in both hard and soft copy, including a CD-ROM version with illustrations.

Less well known, but still popular, are the Sentinel Country Series, which very few people realize is based on the original analysis model developed by the Marine Corps Intelligence Activity in association with Marine Corps warfighters, and provided to Jane's as

an incentive to meet the demand for an unclassified country study. Jane's also publishes a series of extremely detailed reports on defense budgets world-wide.

Not-so-obvious capabilities which every analyst needs to understand are the following:

First, under special arrangements, the full range of information available through Jane's can be obtained online; this can include information on training and maintenance which has not been published and will not be published.

Second, Jane's can undertake special studies on demand, and utilize its special access as well as its in-house store of knowledge to produce useful "proprietary" reports which can serve as the foundation for follow-on all-source studies.

Finally, Jane's has a global network of experts who have spent years studying specific countries and are intimately familiar with specific defense personalities including field commanders. Under appropriate conditions, analysts can arrange to be put in touch with the pertinent Jane's expert, who can then become the analyst's "running buddy" for a specific analysis project.

### **3011. Oxford Analytica**

Oxford Analytica, whose complete range of products is now available to the analyst through the Open Source Information System (OSIS), is believed by many to be the world's best private intelligence agency in the purest sense of the word.

Founded by an American, Dr. David Young, Oxford Analytica was inspired by Dr. Young's experience as the private secretary to Dr. Henry Kissinger when both served on the National Security Staff under President Richard Nixon.

The organization combines a fifteen person "watch team" which is organized by region and reads all the wires each day, with the Dons of Oxford who are rotated through a morning meeting each day, always asking three questions:

- What's right in the news that needs to be expanded for our clients?
- What's wrong in the news that needs to be correct for our clients?
- What "weak signals" are emerging which require a forecast for our clients?

Upon concluding that a special report is required, Oxford Analytica then commissions either a resident Don from Oxford, or one of over 1,000 experts world-wide. In most cases, the experts have direct access to key decision makers and can obtain authoritative insights through a telephone call.

The final unique element of the Oxford Analytica program, strongly influenced by Dr. Young's experience in serving the President of the United States, is that no report is allowed to be over two pages long, and all reports are required to be complete within four hours of commission--as Oxford Analytica is proud of noting, their material is tailored "for Presidents, Prime Ministers, and you".

### **3012. Eastview Publications**

Eastview Publications, a popular provider of services to the Foreign Broadcast Information Service, is representative of the kinds of niche providers that have emerged with the "information explosion" and the opening of formerly denied areas.

It is the foremost provider to the world of military maps from the former Soviet Union, and distinguished itself during the Commission on Intelligence benchmark exercise on open sources by providing, overnight, a listing of all Soviet maps available for Burundi--maps that did not exist in the U.S. inventory and could not have been created by the U.S. for days if not weeks.

Eastview Publications is also a premier source for Russian grey literature, and through its office in Moscow is able to respond to a wide variety of requirements.

Another example of private sector capabilities focused on Russia and Eastern Europe is that of Access International, based in Albuquerque, New Mexico. This organization, managed by Ms. Marjorie Hlava, a distinguished leader of many key U.S. information associations including the American Society for Information Science and the Association of Independent Information Professionals, produces a CD-ROM in both Russian and English on major Russian information sources including legal and technical sources.

In the scientific and technical arena, Information International Associates, closely associated with the Department of Energy Laboratories, the Defense Technical Information Center, and the National Technical Information Service, is one of the best access intermediaries for international information. Ms. Bonnie Carroll, its President, has been a leader in professional organizations such as the National Federation of Indexing and Abstracting Services and others.

The above are only a small sampling of the kinds of capabilities that can help the analyst exploit international sources. Many others exist--for instance, *THIRD WORLD RESOURCES* is a quarterly review of resources from and about the Third World. Ordering information is contained in the hand-out.

### **3013. SPOT Image Corporation**

During the Gulf War, it took just over sixty days to collect the mapping, charting, & geodesy data that was required for both the targeting of precision munitions, and the creation

of 1:50,000 combat charts with contour lines. As U.S. forces are confronted with a variety of contingencies in the Third World--in areas which have not traditionally been high on the U.S. intelligence collection priority list--they are finding that the lack of maps is a critical encyclopedic intelligence shortfall.

Fortunately, the private sector is in a position to make a major contribution in this area. Ten meter imagery from the SPOT Image Corporation, for instance, can be both multi-spectral and panchromatic, and is suitable for creating both 1:50,000 combat charts with contour lines, and three-dimensional mission rehearsal programs. The Air Force also finds it adequate for the targeting of precision munitions.

What SPOT imagery cannot do is provide the "ground truth" precision points needed to ensure accuracy for combined arms operations, and especially for the coordination of artillery and air strikes. This precision is now provided by the National Reconnaissance Office, and can also be provided by human assets on the ground with Global Positioning Satellite Receivers--each SPOT image requires roughly eight precision points (e.g. a precise location for an intersection visible from space), and each country had from 60 to 200 wide area images which comprise its coverage.

The Defense Mapping Agency has made great strides in the past few years in recognizing the value of commercial imagery, and is now in a position to integrate 5 and 10 meter commercial imagery for broad areas, 1 meter imagery for urban detail, and NRO or GPS precision points.

It merits comment that SPOT imagery is the source for project EAGLE VISION, which combine real-time downlinks from SPOT satellites with mission rehearsal software. This project, sponsored by the Air Force Chief of Staff, was used in Aviano, Italy to prepare air crews for flights to Bosnia, and was credited with doubling sortie effectiveness. Commercial imagery is low-cost in comparison to national imagery. in large part because it has a much lower resolution (10 meters versus under 1 meter) and in part because it does not have the security costs associated with national imagery. A normal procurement for a wide area is on the order of \$3,000 to \$5,000; individual "snap-shots" can be had for as low as \$450, and SPOT advertises sales of imagery at \$1.50 a square mile.

### 3014. Universities

Universities, both U.S. and international, comprise a "virtual intelligence community" of great value to the intelligence analyst. Among their unique features are the fact that they focus exclusively on knowledge collection and processing, and that they do so at the expense of someone other than the U.S. taxpayer. University faculty, university student bodies, and university databases are all available to the intelligence analyst at either no cost, or at the nominal cost associated with access to an existing system.



Here are four examples of exceptional facilities of direct utility to intelligence analysts; contact information for each of them is provided in the hand-out:

-- Monterey Institute of International Studies. They have created and they continue to maintain a database on the proliferation of nuclear weapons, utilizing graduate students with native fluency in Russian, Chinese, Korean, Vietnamese, and other languages. Their capability is so extraordinary that they have become the foundation for all-source enhancements within the Nonproliferation Center.

-- Mercyhurst College. This small college in Erie, Pennsylvania is unique because it offers the only program in the United States which grants an undergraduate degree in intelligence and research analysis. Founded and managed by Mr. Robert Heibel, a thirty-year veteran of the Federal Bureau of Investigation, this program requires its students to produce regular newsletters, relying only on open sources, about international narcotics, transnational crime, and other key issues. Students in this program are in very high demand as interns throughout the intelligence community.

-- University of Michigan. They operate a "clearinghouse for subject-oriented Internet resources", including resources for aerospace engineering and government sources of business and economic information.

-- Rice University. They operate an Economic Bulletin Board Service which provides a number of useful files including press releases from the U.S. Trade Representative, defense conversion information, East European trade leads, and so on.

### 3015. Knowledge Age

Knowledge Age, an intended pun, is intended to highlight the fact that knowledge gets old quickly, and to sensitize the analyst to the fact that there are degrees of currency in knowledge which can be very important.

Books are generally ten years old by the time they are published, and many of them started as graduate theses. Magazine articles were generally commissioned and researched ten months before being published. Even newspaper articles, all but the most sensational, were directed by editors and researched by reporters up to ten days before publication. On the Internet, where time moves quickly, clips may be ten hours old.

The point here is that knowledge which has been published is old knowledge.

Where the analyst can get ahead of the curve, and develop insights not yet available to the general public, is by going after unpublished knowledge. By identifying and getting in touch with international experts, the analyst creates the opportunity to ask for tailored new knowledge which is based on unpublished "works in progress".

The analyst should also become sensitive to the existence of "barter networks", and knowledge networks, in which the elite in a particular area of inquiry routinely exchanges insights and information months if not years before publishing. The goal of the analyst should be to establish themselves as a member of this elite, and to use their own unclassified knowledge and their access to unique unclassified information collected at government expense, as their "membership fee" into this broader network of international experts who comprise the analyst's de facto "virtual intelligence community".

### **3016. Conclusion**

There are no hard figures, and in any case the figures will vary from subject to subject and crisis to crisis, but informed judgement is fairly consistent on this point: 80% of what the analyst should know, in the ideal, is not in the USA, is not in English, and is not in electronic form.

The leveraging of international sources is essential for the analyst intent of obtaining a fresh perspective and good "tip-off" value. International open sources and services should be the foundation for a strong all-source analysis program.

## **Chapter 4**

### **THE INTERNET AS A TOOL FOR ALL-SOURCE ANALYSIS**

#### **4001. Purpose of the Chapter**

The purpose of this chapter, developed by Dr. Ross Stapleton-Grey, a former civilian intelligence analyst widely known for his Internet skills, is to present a very broad overview of the global capability known as "The Internet" or "the Net".

The Internet is a global communications medium that permits extraordinary flexibility in communicating with a wide variety of people from all walks of life, in receiving free information from many sources, some of dubious authenticity, and in obtaining access to distributed databases, many multi-media in nature, all over the world.

This chapter will discuss in general terms the utility of the Internet to the all-source analyst, with special attention to the use of electronic mail, newsgroups, lists, and conferencing systems.

We will discuss some of the dangers of the Internet, including the problems of noise and flame wars, as well as the almost total lack of privacy and discretion.

The last half of the chapter will focus on the most productive element of the Internet, the World Wide Web, and will provide five practical examples of how to exploit the Internet in support of the all-source analysis endeavor.

The Internet is a work in progress--it is changing every day at an astonishing rate. Some have characterized it as "the Library of Congress with all the books on the floor". It has its uses, but using it also has its limitations.

This course includes five hand-outs intended to facilitate self-study and hands-on exploration of the Internet's utility as one of the sources for information in support of the all-source analysis endeavor, as well as a source of continuing professional education for the intelligence analyst.

#### **4002. Introduction: What Is the Internet?**

The Internet is a "network of networks" based on standard protocols which have been established by common consensus among international experts. It is unique in that it is not controlled by any governmental body, and is a relatively autonomous, almost anarchistic, system that works because of its common standards.

It began in the 1970's as a Defense Advanced Research Projects Agency (DARPA) testbed to meet Department of Defense research needs and to develop internetworking

technology. It was divested in 1986 to other agencies in the U.S. government, notably the National Science Foundation, with participation from the Department of Energy and the National Aeronautics and Space Administration. The National Science Foundation initially funded regional and national back-bone service providers, and then switched its funding support to end users--this led to the development of commercial service providers. In 1994 U.S. government funding for the Internet ended.

Internet protocols (the standards which allow any computer to join "the Net" from anywhere in the world) won the competition as a general-purpose technology for constructing networks. It's not the most elegant system, and the Internet has a great many faults that other networking schemes avoid (it is still missing a lot of security features), but it is an open protocol, that is, the standards were developed in an open forum. It is now part of every commercial on-line service and computer company's planning because it has become the world's general-purpose digital information carrier.

Most people think of the Internet as a large electronic mail environment. This is its most common use. However, from an analysis point of view it is much more important in its capacity as a global network of distributed databases maintained at the expense of different universities, companies, and individuals. The Internet is an electronic library, with many public spaces and some private spaces.

Commercial services now include data maintenance, data discovery, and--the foundation for future exchanges of content--digital cash. Today, in the absence of wide spread digital cash capabilities, the Internet is largely a direct marketing network, but in the near future it could become the primary vehicle for organizing the exchange of goods and services. The Internet Society is a non profit activity that coordinates Internet standards, but it does not "control" the Internet.

#### **4013. Where Are We Today?**

The Internet is evolving from an academic luxury to a commercial necessity. Today, although the exact numbers are in dispute, we see at least 30 million individual users and over 40 thousand host networks which can be accessed via the Internet.

The Internet continues to grow at geometric rates. Local Internet access providers are finding that they can barely keep up with demand and service is often poor because of the speed with which large numbers of customers sign up daily.

The Internet was fairly closed to users outside government and the universities for much of its history. Big changes occurred when the National Science Foundation (NSF) took steps to turn it from an experimental, research effort, to a commercialized service. The NSF stopped funding networks, and started providing end users (such as schools) with funding to buy network services, establishing the first competitive markets for Internet services. Growth has been enormous ever since the NSF established regional networks (such as SURANET in

the Washington D.C. area) and especially since most of the restrictions (such as NSF's "Acceptable Use Policy" for its networks that required traffic be noncommercial research and academic in nature) were removed.

Today over 50% of the Internet sites are commercial in nature, with research organizations including universities comprising another 29%.

There is less "content" than one might expect. One authority, Dr. Joseph Markowitz, Director of the Community Open Source Program Office, notes in his primary briefing on open sources that "content" comprises just one percent of the Internet, with electronic mail, advertising, and other uses occupying 99% of that capability.

*"The Internet is like the Library of Congress,  
but with all the books strewn randomly on the floor."*

This popular quotation, in several variations, has been around for years, but no one, including Dr. Vint Cerf, founder of the Internet and most recent President of The Internet Society, knows just who first thought of the analogy--but it is a good one!

#### **4004. How Representative Is the Internet?**

There are three ways to understand the character of the Internet.

In global political terms, it is dominated by the United States of America, which has more users, more hosts, and more bandwidth than the rest of the world taken together. Western Europe is a very weak second to the USA. The major online service providers, American OnLine and Compuserve, are U.S. companies with a global membership.

In most countries, only a relatively small number of prominent scientists or wealthy users are able to access the Internet, and many of them are restricted by local telecommunications limitations to a very low baud rate and a short access time. This represents the technical character of the Internet. In much of Africa, Asia, and Latin America, for instance, technical constraints are severe.

The Internet became a popular phenomenon around 1994, and exploded on the commercial markets in 1995. Online services all established connections to the Internet, so many of those users can be considered to be "on the Internet." However, it is very important for online service customers, such as those using America Online and Compuserve, to understand that the access they receive to the Internet from these services may be constrained-- Internet search tools such as Web Crawler will "see" only those Internet sites that have been registered by the managers of the online services. Analysts using the Internet need to understand what "hidden limits" might be placed on their searches and the search results by such constraints.

Examining the Internet at a personal level, the overwhelming majority of users around the globe, i.e. factoring in all countries, is comprised of research scientists. Within the USA, on the other hand, the largest group is individuals for whom the convenience and low cost of electronic mail and conferencing has become a major attraction. A third kind of user, the organizational user, is being provided with Internet access as a means of reducing organizational communications costs and increasing informal coordination among members of the organization.

#### **4005. Lists: Versatile Low-Tech Tools**

Electronic mail is the single most familiar tool on the Internet. Distribution lists are a first step beyond simple point-to-point E-mail. Analysts can quickly create their own individual "broadcast" groups that permit them to share information or ask questions of their counterparts world-wide.

Automated Lists, known as "Listservs" can be moderated or open. Such lists maintain a constantly changing directory of interested parties, and re-broadcast any messages sent to them to all current members of the list. Membership can be restricted, or open

Electronic mail is the lowest common denominator, since it can be used from virtually any platform (including dumb terminals) and doesn't need to be real-time. Usually one or more individuals interested in an issue or topic will create a distribution list as their set of correspondents grows beyond a few dozen. Some mailing lists may have thousands of subscribers.

Three examples of listservs of interest to the all source analyst are the Open Source List, maintained by the U.S. Army's 434th Military Intelligence Detachment (Strategic); the C4I List maintained by the Naval Postgraduate School, and the Information Warfare List, maintained by Dr. Fred Cohen, an international authority on information warfare who has served as a principal investigator for many defense and intelligence projects. Information on subscribing to all three lists is provided in Appendix E-2.

If you cannot find a list that meets your needs, consider starting your own--you could create one within the classified environment, and another within the open source environment. If you do not wish to be burdened with the maintenance, consider contracting this task out to a related center of excellence, such as a university with a strong program in your regional or functional area of interest.

A complete discussion of listservs and how to find and use them is provided as Appendix E-4.

#### **4006. USENET and Its Newsgroups**

USENET is a collection of thousands of newsgroups. Newsgroups are much like

E-mail distribution lists, focused on specific topics and with an emphasis on current events. Internet hosts pass each other USENET "feeds". USENET is not be confused with the larger Internet, something which happens frequently among new users.

USENET newsgroups are similar to bulletin boards, but require special newsreader programs to access the material. Instead of having mail arrive in the user's mailbox, the user accesses postings being held on a server, which is something like using a bulletin board system over a network.

Analysts contracting for an online service should note that in those instances where the basic membership only covers a few hours a month, and there are additional charges for any more time on line, it can become very expensive to do news reading online. One simple way to reduce costs is to utilize the "capture" feature in the communications software, and set for screen scrolling when entering the news area. This will allow for off-line reading as well as cutting and printing, and reduce online time to a minimum.

Here are three examples of pertinent newsgroups; a listing of typical headlines from each is contained at the end of Appendix E-1:

< soc.culture.kuwait >  
< alt.current-events.bosnia >  
< alt.politics.org.us >

Newsreader programs are generally provided by the same service through which you obtain access to the internet. They are all generally similar.

#### **4007. Conferencing Systems**

Conferencing systems are organized discussions, and are hosted on a server or servers which allow authorized participants, those who have password access to the system, to create conferences and within conferences, topics. All other users then have the option of reading entries, contributing their own entries, or "forgetting" the conference or topic by marking it as not being of interest.

Both Compuserve and America Online can be thought of as conferencing systems that "grew up;" when they first began members could only exchange information with other members, using both E-mail and public postings. As the Internet began to become an attractive resource, there was a great deal of pressure on the online systems to tie their services to the Internet, or risk loss of their members to ones that did. Some of the conferencing systems police their content, as Prodigy (to ensure that it's "family friendly") and America Online (which calls its rules its "terms of service") do. The online services do face some policy dilemmas, though: the Stratton Oakmont legal case ruled that because Prodigy censored some members' postings they could be held liable for not censoring libelous postings.

An examples of a Compuserve conference of possible interest is the Military Forum, which you reach--if you are a Compuserve subscriber, by typing "GO MILFORUM". Compuserve provides a number of other services of possible interest to analysts, including "GO MAGELLAN", where maps of current hot spots are available in GIF format, free, and other maps are available for a fee; "GO MAGDB", a large collection of journal articles; and "GO ENS", where ENS stands for Executive News Service, and permits you to establish a profile that selects articles of interest for your personal mailbox.

In the Whole Earth Electronic Link, possibly the most well-known and respected conference system ever built, topics 268 and 288 in the Whole Earth Review conference focus on open sources of intelligence and the reinvention of intelligence. Like most conference systems, monthly subscription fees are required to gain access.

#### **4008. CAUTION: Some Problem Areas**

Lists, newsgroups or conferences are contributed to and seen by hundreds to hundreds of thousands. The "noise to signal ratio" on the Internet is very high. If one subscribes to too many lists, or becomes too well known, they can be flooded with information. Although there are some sophisticated tools available today to help filter incoming information, one crude technique is to maintain several electronic identities, including an "unlisted" identity for personal friends. Another technique is to file everything, and then search for specific items of interest within this more limited (but still large) pool of information.

Another problem on the Net is that of "flames" and "flamers". Information on lists, USENET, conferences comes from broad communities of individuals. Although closely moderated lists may produce a high ratio of "wheat" to "chaff", many unmoderated discussions collapse under the weight of a few disruptive sources. "Flame wars" (harassing postings, name calling, and generally disruptive noise) are also common. Some contentious political and ethical discussions (such as on abortion, religion, race, etc.) are guaranteed "flame" generators. Analysts examining newsgroups and posting pertaining to the Middle East or the Balkan region are likely to find diverse and strong opinions, and have some difficulty sorting usable information from personal opinion.

It is important to understand that virtually anyone could be posting the materials found on the Internet, and that it will often be hard to ascertain the credibility of the source. Tools exist to explore "who is" a particular poster, and very good biographical information can often be obtained--as provided by the source themself.

Search tools and online services have their own limitations. Some Web search tools are best for thoroughness, others for new material, others for finding related information that does not have the actual key words. Searching the Net through an online service rather than a direct access provider will severely limit your results because online service providers impose censorship and access restrictions.



Everything about the Net is open for scrutiny by anonymous lurkers who can watch everything you post without revealing their presence, and in some cases arrange (illegally, or by abusing their authorized access as service providers) to monitor your private electronic mail. Internet users need to understand that there really is no such thing as private mail--an electronic message is forever, and might be seen by anyone!

#### **4009. How On-Line Communities Form**

It only takes two people to form an online community and share information. Word of mouth and existing personal relationships can quickly expand such communities. The practice of forwarding electronic mail to others is a very low-cost way of sharing information, and leads to widening communities. Broadcasting messages to lists of known interested parties also strengthens communities.

Users with common interests join (or create) lists and newsgroups. Their public postings are advertisements for communication, and users respond to each others' postings. Lists can be attract participants with very specific interests, e.g., C41.

"Face to Face" communications are an essential aspect of online credibility and sustainability. At some point individuals will want to meet professionally, and this may strengthen or weaken the willingness to invest time online.

Given the face to face rapport, however, and a desire to share information, online communications quickly proves to be better than voice (you can send and forget electronic mail or have it cheaply translated enroute), it is cheaper than voice, and it provided an automatic record of exchanges.

Whether or not a professional and official email address is provided to the analyst, a personal email address through a commercial service provider is a good investment, both for personal communications with relatives and friends who are increasingly turning to the Internet as a primary communications channel, and for professional browsing in the open source world, where a great deal of information can be legally and ethically examined and downloaded without revealing your interest or your organizational affiliation. Analysts must ensure they follow approved procedures when integrating open source digital information into their all-source digital environment. The easiest and safest means is to keep external open source material in printed form, and to scan or keyboard pertinent passages. The alternative is to provide a diskette or send an electronic file to the authorized security point of transfer. Do not take chances with open source digital data!

#### **4010. On-Line Communities, Virtual Contacts**

The Internet community has literally exploded in the 1990's, and one can quickly find an online community for just about any topic. Not only are there

many, many pre-existing communities, but the conferencing systems spawn new ad hoc communities every day to deal with current events.

Such communities are a first step in identifying experts who can then be cultivated directly through "off line" personal electronic mail or more formal communications. An analyst can quickly build a "short list" of key people whose commentary can be observed and evaluated from a distance, as a "lurker", before ever introducing one's self. Networking informal sources to get a "head start" on an analysis issue is one of the best possible uses of the Internet. Remember, these communities of experts have spent decades of cumulative time becoming expert in specific areas, and they are usually going to be more familiar than the analyst with other experts and open sources of information about the topic or issue. They can provide a "first cut" that might otherwise take weeks of expensive library research.

There is an Internet culture, and there are standards of behavior. Although, as the New Yorker cartoon of two dogs dramatizes, "on the Internet, no one knows you are a dog", in fact first impressions matter and people will quickly form an opinion as to whether you are abusing their time, contributing to the discussion, or being stupid. Building trust on the Net takes patience, maturity, and a willingness to make constructive contributions to whatever discussions are important to you.

The Internet is today largely a barter or gift economy. At one meeting of international hackers, it was generally agreed that for every piece of information they each contributed to the Net, they generally got 100 pieces back, of which 10 were useful--hence a 10 to 1 noise ratio, but also a 10 to 1 return on investment.

Analysts who are cruising the Internet for information need to be aware of and comply with whatever official constraints may apply. If in doubt, don't post--just lurk and download, use the Internet as a cheap background briefing. The analyst also has the option of using the Internet, together with other traditional research tools such as the *Social Science Citation Index* and the *Science Citation Index* published by the Institute for Scientific Information, to identify possible direct contacts for official approval.

#### **4011. Structuring Knowledge: Tools and Trends**

Gopher was the first, popular tool for moving beyond lists and searching for information. The command, used at the prompt with the name of the site which must be known in advance, allows the analyst to access embedded menus and to select items to be downloaded. The Veronica search engine was created to search across a multitude of poorly documented Gopher sites. As gopher sites are now almost extinct, this is mentioned primarily as background.

WAIS was, until the World Wide Web, developed, the Rolls Royce of search engines, and for the first time provided a reliable means of both weighing the relevance of the found

files, and also of refining searches by commanding it to look for other documents "like" documents already in hand and found to be valuable.

Today, the two most popular tools are Netscape and the Web-Crawler. However, tools for the Internet are literally "exploding". Besides WebBrowser and the Microsoft Internet Explorer, the most impressive new tool, not yet widely used by the average individual, is Alta Vista, from Digital Equipment Corporation. Where the four programs return between 20 to 2000 "hits" on the name "Bill Gates", Alta Vista powers through the entire Internet and identifies 80,000 hits! Directions for using each of the above programs are found in the first student hand-out, together with other useful information for exploring the Web. Two of the hand-outs list specific sites of value to the intelligence analyst.

The Internet has always had an information organization problem, since very few people have ever been paid to create catalogs or indexes, there are few standards for online citations, and a great many documents and resources have just been dumped onto Internet sites with little regard for documenting their origin, validity, or even date of creation (much less expiration). Although commercial providers can be expected to offer value-added discovery and discrimination tools of increasing sophistication, it is difficult today to replicate a search, and most experienced navigators find that their best aid is a logbook in which they keep meticulous track of their wanderings in cyberspace. "Bookmarks" are citations of Web sites that a user can save, allowing them to find their way back later--the bookmarks are saved locally, and constitute a personal "map" of key terrain in cyberspace. Organize your hard drive and save the good stuff. Use your electronic mail program, such as PINE, to maintain electronic files with copies of messages from key contacts sorted by topic or area of expertise.

#### **4012. The World Wide Web**

The World Wide Web is a true multi-media environment which moves well beyond Gopher's linking of documents and sites, to allow true "hypertext" and "hyper-linking" of images to sounds, sounds to text, documents to other documents, and sites to other sites.

Readers can jump from the middle of a document to some supporting or related document, navigating the Web just like they might move through a library, pulling a reference volume off the shelf upon encountering an unfamiliar term. The Mosaic browser made the Web extremely easy to use, and the work that went into Mosaic was used to create the Netscape browser, which led to the creation of a billion dollar company.

The biggest problem with the Web today is that because it is multi-media, it is a band-width hog, and the demand for access is overwhelming most service providers. There will probably be a slow-down in the Internet in 1996, because a new performance plateau is achieved by the industry.

Users of the Web environment also require a special kind of Internet access, called SLIP, rather than the normal electronic mail and gopher text capability.

Appendix E-1 contains details instructions on how to explore the Web, and how to use different tools.

Here are four examples of useful Web sites. The first is a site dedicated to providing information about different countries; the second focuses on open sources and methods, and includes a full year of its newsletter; the third is a current news service focused strictly on the intelligence profession; and the last is the main access point to all federal government databases and bulletin boards that are accessible to the public.

<www.embassy.org>  
<www.oss.net/oss>  
<www.awpi.com:80/IntelWeb/>  
<www.fedworld.gov>

#### **4013. Where the Web Has Been, and Where It's Headed**

The Web relies on Hypertext Markup Language (HTML), which in turn is an open and evolving document creation standard that will permit new applications to work on any standard document.

While running a Web site is technically demanding, many companies are now providing Web space (called a Home Page) for users, just like management companies buy and rent space in commercial buildings. Individuals have the option of hiring a "virtual" server" and obtaining their own domain name, such as "ANALYST.COM".

Security is an issue. Many Web servers do support secure connections, so a user can be sure that the information passing between his or her browser and the server is confidential important when passing credit card information, or other sensitive personal information. Password access can be complicated, so today most home pages and web servers are "wide open".

The next step will be for widely accepted commercial transaction standards to emerge; when this happens we're likely to see it happen quickly, just as point of sale (POS) devices (e.g., credit card swipe readers) have appeared at most retail stores. Digital cash, called by some "cyber-cash", is likely to be commonly available by 1997.

Popular Web sites attract thousands of users per day, and many include advertising graphics on their sites, being paid by the number of "hits" or "page views" they guarantee advertisers. Several companies provide auditing services to verify how much visibility sites provide advertisers.

The Web is likely to make virtual consulting by individual a real possibility, and permit many experts to establish part-time or full-time "cottage industries" selling their expertise to people all over the world in return for digital cash. This is like to cause a number of governments great concern, and may lead to a "virtual taxation" regime--the latter, will however, be very difficult to impose in a world where many encryption alternatives are available.

The professional analyst should think of the Web as a virtual collection environment, where Web sites can be established, and good content provided, as a means of drawing out expertise and collecting both fact and opinion about the topic in question.

#### **4014. Finding Information on the Web**

Like the earlier favorite Gopher, searching for things has led to the creation of special search sites. Some sites are important clearinghouses for links to other sites. Several very powerful full-text search sites have been established.

Four examples, each fully described in Appendix E-1, are listed here.

Yahoo:	< <a href="http://www.yahoo.com">http://www.yahoo.com</a> >
Alta Vista:	< <a href="http://altavista.digital.com">http://altavista.digital.com</a> >
InfoSeek:	< <a href="http://www.infoseek.com">http://www.infoseek.com</a> >
Open Text:	< <a href="http://www.opentext.com">http://www.opentext.com</a> >

Analysts must naturally be concerned that any search they make might reveal a classified interest, but in reality, most analyst is responding to current events and the analyst can find security in obscurity. Everyone else is searching the same sites at the same time. As long as the analyst is searching and not posting, a very reasonable degree of discretion can be assumed.

The appendices corresponding to this chapter are your best guide to finding information on the Web, and contain a great deal of information which could not possibly be communicated in this short one-hour course.

Explore the Net, and keep a log-book. The Web discovery tools also provide "bookmark" features which allow you to keep a list of especially valuable sites to which you can return regularly.

#### **4015. "Intranetting"**

Many companies are concerned about security and create their own internal networks, hiding behind firewalls, which are ostensibly "total" breaks between the internal system and the external Internet.

Intranetting is an important consideration to note, because while such information won't be accessible to the public at large, sources and contacts met through the Internet may themselves have access. An analyst can thus obtain access in only two ways. by being an authorized internal user of the system in question, or by going through a personal intermediary, an authorized liaison, who can conduct internal searches and then transfer to the analyst the resulting data.

Examples of two intelligence community "intranets" are INTELINK and OSIS.

INTELINK is a classified Internet; that is, the Intelligence Community has built a secure copy of the Internet for sharing information, with the ease and efficiency enabled by use of World Wide Web servers and browsers, but in a classified setting. In this case, the "firewall" is an air gap. with no direct connections to the global unsecure parent.

OSIS, standing for "Open Source Information System", is a "virtual private network", where several intelligence agencies use the Internet itself for sharing unclassified information more easily, but software, in the form of firewalls and filters, keeps this traffic apart from the rest of the Internet.

Some of the best information available is hidden from the Internet in private intranet environments. This includes both university and corporate data. Analysts need to identify centers of excellence and then explore how they might obtain authorized access to the available data even if it is not directly accessible through the Internet.

The whole area of "intranetting" demonstrates the critical importance of personal networks--the analyst that identifies and cultivates a network of experts will find that the personal contacts can identify and gain access to data regardless of whether it would have been identified through an Internet search--and the Internet will often be the vehicle used for communicating with those experts, and receiving file transfers from them.

#### **4016. Practical Example #1: Indications and Warning**

In each of these four cases, information was quickly shared over the Internet, though in several of the cases the information was also traveling through more traditional means.

Researchers at a Swedish university have published a two-volume set of excerpts from network traffic around the Tiananmen Square incidents, including notes calling for protests at Chinese diplomatic facilities in the West, and information passed out of China via fax and phone (and carried by hand) and resent through E-mail. An analyst following Chinese newsgroups is very likely to have been alerted to these events prior to official reports from the U.S. Embassy or other collection capabilities.

Similarly, details of the situation in Moscow during the coup attempt against Gorbachev and Yeltsin were broadcast over the Internet (Yeltsin used a fax to get his statements to the Western press, however, and Gorbachev taped a statement about his detention using his VCR).

The Intel Pentium problem demonstrated the Internet's power as a consumer awareness channel: the bug that Intel considered minor (it only affected the work of serious mathematical processors) was blown up into a major public relations issue. It did however have significant financial ramifications for Intel stock. Similarly, other corporate or technical news can be studied for tip-offs.

Mathematicians have been using the Internet for the past several years to coordinate attacks on complex factoring and other problems, and their achievements have been widely announced via the Internet as solutions are found. On the other hand (and reminding us of the need for caution) the bogus "cold fusion" research was also spread via the Internet, attracting far more attention than it merited.

#### **4017. Practical Example #2: Cultural Context**

The Internet is a rich resource of information on distant countries and cultures. Because it's an open channel for information from virtually anyone with access to E-mail, it can become choked with both information and disinformation, but it's hard not to be able to find something on virtually any topic.

At the very end of your first hand-out you will find some extracted lists of messages and files pertaining to Kuwait, Bosnia, and the United Nations.

In combination, newsgroups, listservs, and web sites provide a rich background about current events and historical context. These passive sources of information--passive in the sense that you can "lurk", also permit analysts to rapidly identify articulate individuals to whom "off-line" questions can be posed, saving the analyst significant research time by providing a local perspective and a sense of a situation that would otherwise require hours of reading and might never result in the kind of insight that can be obtained from someone who is heavily involved in the issues under consideration.

#### **4018. Practical Example #3: Basic Research**

While the Internet covers a broad spectrum of exotic information, it's also a good repository for basic information.

Some of the first information resources were library card catalogs (catalog databases were simply connected up to allow searching via the Internet); any other product that could be placed on a disk or CD-ROM might also be placed on a Web host.

Appendix E-2 lists a wide variety of sites especially pertinent to intelligence analysts. Appendix E-3 focuses on popular web sites covering computer resources, news, government, and reference. Examples from both lists are shown here.

MILNET: Open Source Military Information Database  
Military Intelligence: 20th Special Forces Group  
CIA Country Reports  
Department of State Country Reports  
CNN Interactive  
Reuters NewsMedia  
Library of Congress  
Britannica Online

#### **4019. Practical Example #4: Science and Technology Collection**

Virtually every area of interest can be found through the web and listservs. Every analyst with an S&T aspect to their work should consider searching for selected sites and also subscribing to selected listservs in their areas of interest.

Appendix E-2 lists a number of sites associated with weapons transfers and information warfare, some shown here.

High Energy Weapons Archive  
Germ Warfare  
Code Names and Numbers for Weapons  
IW Database  
Defense Information Systems Agency--Information Security  
Computer Security Institute

Appendix E-3 lists a starting point for scientific and technical information, elements of which are shown here.

Biographical Information  
Directory of Scientific Institutions  
Electronic Journals

#### **4020. Practical Example #5: Spotting and Assessment**

The Internet is both open and public, and capable of allowing private communication. As users interact on mailing lists, newsgroups and conferences, they are seen (or read) by others. Estimates are that roughly 90% of the members of most conferences or newsgroups are "lurkers," that is, only read, and never contribute materials of their own. But a visible poster may attract private E-mail, volunteering information that the sender would like known, but wouldn't be comfortable posting directly.



You can often bait the hook, by offering (sincerely) to exchange information that you are authorized to share without violating copyrights. Sometimes your personal impressions as a professional analyst, and copies of articles that you have published in the unclassified literature, are enough to attract your counter-parts into dialogue.

Occasionally you may find yourself dealing with an electronic walk-in, someone who is volunteering information which appears credible and which may also be subjecting the individual in question to some risk if discovered. Such cases should be brought to the immediate attention of HUMINT and counterintelligence through established channels, not to give them up, but to ensure that the analyst has a full range of HUMINT and CI assistance in developing the source or--in some cases--turning over the source to a clandestine case officer.

Analysts who find names and backgrounds of interest always have the option of requesting security traces through channels. Working with HUMINT professionals can be a rewarding way of furthering any analyst's understanding of the network of human experts available to support the all-source project. Analysts can help the HUMINT discipline by identifying high-value targets for clandestine recruitment, and at the same time receive HUMINT assistance and cooperation in developing approved overt human sources, for whom funds can be budgeted.

#### **4021. Second Caution: Mischief in Cyberspace**

Because of the "faceless" nature of the Internet, it's possible to make mischief, from harassment to propaganda on a grand scale. "Astroturf" and "whisper campaigns" are where a few individuals (or even a single individual) can create numerous postings, attributed to a great many more people, in an effort to create a seeming consensus toward an issue or candidate.

"Spamming" occurs when an individual sends numerous and inappropriate postings to large audiences, through numerous mailing lists or newsgroups. This is at best annoying, and can, at worst, severely disrupt recipients' systems, choking their Internet connections or incurring significant costs if they have to pay by the volume of information received.

Because there are few if any restrictions on the collection of information from Internet search tools, and one should presume that, unless encryption is used, communications over the Internet can be at least noted, if not intercepted, one should be concerned about traffic analysis (on the other hand, if one owns a search tool site, one can readily gauge what issues Internet users find interesting!).

Trojan horses and viruses are malicious code that could be placed in resources made available on the Internet; while troublesome, they can be easily avoided by scanning any downloaded software, or limiting collection to text only. Analysts need to be aware that

icons are now also known to be active, and executable code can in fact be imported when importing "non-executable" data and graphics.

#### **4022. Pulling It All Together**

This one-hour introduction to the Internet as a tool for all-source analysis has provided you with an overview of various tools and sources you can find on the Internet.

Here we show a sequence of steps which an analyst can pursue to exploit the Internet in support of a specific project.

- |         |                                     |
|---------|-------------------------------------|
| Step 1. | Search for Background               |
| Step 2. | Identify Experts                    |
| Step 3. | Identify Lists and Newsgroups       |
| Step 4. | Send Some Electronic Mail           |
| Step 5. | Post Some Queries on Conferences    |
| Step 6. | Establish a List or Web Site        |
| Step 7. | Host a "Face to Face" Working Lunch |
| Step 8. | Contribute Unclassified Information |
| Step 9. | Develop Collaborative Relationships |

An initial Web search can readily identify background documents. Together with a search of newsgroups and listservs, a number of experts commentators can be identified through their public postings.

Depending on the sensitivity of the query, the analyst can then take an active role by sending selected electronic mail or posting some general queries. Analysts should be mindful of Net protocols and the general expectation of the barter environment which characterizes the Internet—a sense of professional sharing and the expectation of exchanged favors.

At a more sophisticated level, analysts can work with appropriate infrastructure personnel to create a list or web site focused on their specific interests. This can serve as a magnet for individuals world-wide. In the early stages of the list or web site, it is useful to "salt" it with an introductory document that is deliberately loaded with "hot" words or keywords. Also, it is important to note that direct contact with the more popular clearinghouses can ensure that the site is properly listed and described.

Finally, the analyst can use the Internet to keep in touch with specific individuals, to coordinate face to face meetings, and generally to develop collaborative relationships with private sector peers eager to share unclassified information.

#### **4023. Anticipating Coming Changes**

Electronic commerce, as it arrives, will limit some formerly open resources (as people begin to charge what they'd had to previously give out for free) but will also help to fund efforts (such as cataloging) that are sorely needed, and will let others feel comfortable putting new resources online. As the volume of materials become such that most information needs can be met via the Internet (one-stop shopping) such catalogs and directories will become critical.

Since human searching is a chokepoint (there's only so much one person can scan through), we'll see tools for automating searches, or even turning them over to software "agents" to do the heavy lifting of browsing through hundreds or thousands of sites in search of relevant materials.

We've already seen some restrictions on Internet content, such as bans on "indecent" content. Some countries have much stricter restrictions on speech than the US, but the Internet, as a global system, will challenge attempts at censure. Access will continue to expand, especially to let travelers more easily access the Internet when away from home or office.

Some things, however, will NOT change. Analysts will continue to encounter a world of knowledge in which most of the information they really need is in hard-copy, is in a foreign language, and is somewhere else. In all these cases, it will be people who can help the analyst discover key data, discriminate between good and bad data, and distill masses of data into raw information which can then be considered by the analyst as part of the all-source intelligence process.

#### **4024. Conclusion: A Work in Progress**

Not only has the Internet changed dramatically over the last several years, the rate of change appears to be increasing. Commercialization is likely to cause further bends in the curve, as it will suddenly become possible for easy electronic sales of information, creating incentives both for companies to put resources online, and for others to create indexes and catalogs to those resources. Low cost global access and virtual conferencing are a rapidly approaching reality.

The Internet isn't the sum of all the world's information, but it is a good jumping off point, and grants easy access to potential sources and experts worldwide. It can also provide new avenues of access to traditional intelligence sources, e.g., as a spotting and assessment tool. It certainly allows activities that would have been impossible previously because of time and distance (such as convening a panel of experts on a fast-breaking topic), and will only improve in that regard as most potential participants in such activities get online themselves.

The analyst's access to both raw data and alternative perspectives is growing quickly because of the Internet; analysis will never be the same. However, the process of analysis has not changed--in evaluating the potential contributions of the Internet to the all-source analysis process, the analyst must remember security, remember source authentication, and remember completeness.

## Chapter 5

### OPEN SOURCES AND MILITARY CAPABILITIES

#### 5001. Purpose of the Chapter

This chapter focuses on the practical application of open sources to military intelligence analysis requirements.

We will begin by introducing a model for integrated all-source analysis which illustrates the critical importance of geographic and civil factors in evaluating the threat at each of the levels of analysis. While open sources are useful in conducting research and developing intelligence estimates about military capabilities in isolation, open sources are most useful to the military intelligence analyst when used to develop a broader analytical model.

The general utility of open sources for military intelligence analysis, and the specific utility of open sources at the strategic, operational, tactical, and technical levels of analysis will be discussed.

Next we will look at specific private sector capabilities for collecting and processing open source information. Commercial imagery, private sector order of battle information, and networks of experts available for consultation will be reviewed in general terms.

Finally this chapter introduces the student to the Expeditionary Factors study developed by the Marine Corps Intelligence Activity, and used for this class because it is the only current and authoritative intelligence analysis product which relies exclusively on open sources, is unclassified in its final form, and covers a broad range of mission area factors for eighty countries specifically chosen because of the likelihood that a Marine Air Ground Task Force will be engaged in non-combatant or combatant missions in the countries

There are three Appendices associated with this chapter--Appendix A, which was introduced in Chapter 1, and Appendices F-1 and F-2.

#### 5002. Model for Integrated All-Source Analysis

The four levels of analysis first popularized and thoroughly explained by Edward N. Luttwak in his book, *STRATEGY: The Logic of War and Peace* (Belknap, 1987), are most easily understood with an illustration. The Marine Corps Intelligence Center expanded this model by distinguishing between military, geographic, and civil factors. The third hand-out is a complete description of the model, including a summary illustration on page v.

When the model was first developed, a specific Middle Eastern country was used by the Marine Corps, in consultation with DIA, CIA, and NSA analysts responsible for that

country. to test assumptions. Their tank warfare capability, traditionally assessed as a high threat, proved on examination through the four levels of analysis, to be a high threat only at the technical level, because the country had an inventory of T-72 tanks, the best tanks that money could buy at the time. At the tactical level of analysis, the threat dropped to low because the tanks were not being maintained, in fact were being cannibalized for parts, and the troops were not trained. At the operational level, the tank threat increased to medium because there were a significant number of tanks available around the country. Finally, at the strategic level of analysis, the tank threat again dropped to low because it was not possible for the country to sustain tank operations for very long.

This analytical model becomes even more useful when we introduce the three analysis domains--military, geographic, and civil--and consider how the three domains interact at each level of analysis. At the strategic level, military sustainability, geographic location, and civil allies are the essential elements of employable power. At the operational level, military availability, geographic resources, and civil instability bear on the regional influence of the target country. At the tactical level, military reliability, geographic terrain, and civil psychology come together to determine battlefield dynamics. Finally, at the technical level, military lethality (and accuracy), geographic atmosphere--specifically temperature--and civil infrastructure including communications and computing systems, help determine the balance of power.

In short, the threat varies depending on the level of analysis. Open sources provide both raw information, and a general context, for this more complex form of analysis.

### 5003. General Utility of OSINT

There are three major ways in which open sources are very useful to the defense intelligence analyst:

First, open sources are very quickly and cheaply available, and even when the full weight of the traditional classified capabilities are being brought to bear, will offer the analyst--and the supported policy maker or commander--a rapid orientation useful for planning purposes.

For example, in one case where U.S. forces were being directed to deploy quickly to a remote area of Turkey, it was an open source reference which quickly identified the nearest airfields and their runway, navigation, and bunkering capabilities.

In many cases, open sources may be the only available source for a significant period of time. As military operations other than war, and unanticipated contingencies, tend to occur in Third World countries that are Tier 3 or Tier 4 in terms of standing intelligence priorities, it will often be the case that the military intelligence analyst and the operating forces will be forced to rely exclusively on commercial imagery, private sector news broadcasts, and direct contact with overt human experts, in order to produce intelligence.

The second area where open sources have a significant value is with respect to collection management. By providing a rapid and inexpensive orientation, a "first cut" on what is known and what is not known, open sources has enable the analyst to develop a collection management strategy which avoids wasting precious classified resources of essential elements of information which can be handled by open sources, and which focuses the clandestine and technical capabilities on "the hard stuff".

Finally, open sources are very helpful when conducting joint or coalition operations, including support to law enforcement, where there are constraints on the sharing of classified intelligence, and it is considered prudent to avoid sharing sensitive intelligence and the means by which the intelligence was obtained.

#### **5004. Strategic Intelligence**

At the strategic level, military sustainability, geographic location, and civil allies are critical elements of national power. Much of the information needed at this level is in fact available through open sources.

In the indications & warning arena, open sources can--through the technique of content analysis and comparisons of content over time--provide very reliable gauges of national intent. In fact, the Office of Strategic Services and its original Research & Analysis Branch made the analysis of open sources an art form--by studying what the German leaders were telling their own people through the public media, the OSS was able to develop estimative intelligence.

Open sources are also critical in two areas traditionally not within the normal scope of classified systems--demographic intelligence and cultural intelligence. Today, as organizations such as the U.S. Information Agency begin to apply intelligence methods to open sources, and adopt a collection and reporting role in these areas (as was recently recommended to their oversight body, the U.S. Commission on Public Diplomacy--the analyst may find that one of their most important sources for partially analyzed open source information is the traditional consumer of intelligence.

Strategic generalizations are not yet a well developed aspect of national intelligence support to acquisition, but as the concluding chapters will demonstrate, a potentially important means of money and improving system performance. To take just one example: if aircraft are built to a standard "warm" day, and the "real world" of contingencies is in fact a "hot" world, then by definition our forces will be using aviation resources which can fly half as far and carry half as much as advertised when operating at the "optimal" temperature. When European truck manufacturers adopt a strict policy of never selling a vehicle weighing over thirty tons to a Third World county, the viability of some of our heavier ground combat vehicles must be called into question.

At the strategic level open sources are helpful in understanding the context for security assistance programs, and in developing support for specific programs from the public, the press, and the policy community.

#### **5005. Operational Intelligence**

At the operational level, military availability, geographic resources, and civil instability influence the regional effectiveness of individual countries.

It is very helpful for an analyst to develop regional generalizations, to establish an understanding of order of battle averages, and of geographic and civil constraints characteristic of the region. Third World operations are inherently different from the European theater operations against a Soviet threat for which most U.S. mobility and weapons systems were designed--the analyst that understand both the limitations of our own systems in the Third World, and the possible advantages which accrue to those fighting on their home ground with equipment designed for their home ground, will probably produce more useful intelligence products.

Open sources are especially valuable to the theater commander and those supporting the theater and its Joint Intelligence Center because most contingencies will not warrant major collection campaigns from classified sources. This is true both in the planning phase, and in the execution phase when it is necessary to coordinate logistics and other matters with joint and coalition partners. At the operational level, where the greatest mixture of allied and U.S. services is to be found, and there is a greater involvement of civilian agencies from both the U.S. and other countries, secrecy can be an impediment to understanding and consensus, and open sources can have a corresponding simplicity which increases cooperation and improves coordination.

As the theater staff plans the allocation of resources, a sound understanding of the region and the capabilities of all parties to the operation, largely gathered through open sources, can help determine what should be left on the pier, what additional capabilities are needed from the national level, and what to expect or request for allies.

#### **5006. Tactical Intelligence**

At the tactical level, military reliability, geographic terrain, and civil psychology are essential determinants of battlefield success.

At this level, where combined arms coordination at the 1:50,000 scale is essential to the art of maneuver and the control of precision munitions, commercial imagery is often the only available source which can be brought to bear. National collection capabilities are not well-suited for wide area surveillance, they were designed for point targets, and will naturally be much in demand for the development of target intelligence.



Commercial imagery, notably SPOT imagery at the 10 meter level of resolution (meaning you can see an object ten meters wide on the ground), is not only fully suitable for the creation of 1:50,000 combat charts with contour lines, but has also proven to be more than acceptable to the U.S. Air Force as the foundation for targeting precision munitions, and as the source for digital elevation data used to create sophisticated simulations for mission rehearsals and other needs.

It is important to note that commercial imagery requires the addition of "ground truth" points to orient the image and establish precise geo-spatial accuracy. Such precision is obtainable in two ways: through the integration of precision points (e.g. key intersections) obtained from the National Reconnaissance Office through the Defense Mapping Agency, or through Global Positioning Satellite (GPS) recordings taken by human assets actually on the ground.

Open sources are very useful in emerging target areas which have not been heavily covered by classified capabilities. The Director of the Non-Proliferation Center, for instance, has stated publicly as much as 80% of his final intelligence products are based on open sources; in counter-narcotics operations, open sources--including investigative journalism in Latin American newspapers--has proven to be accurate and comprehensive....so much so that the U.S. Southern Command enlisted the Department of Energy laboratories (Los Alamos and Sandia) to collect and process open source information from Latin America, with the result that tactical interdiction operations were mounted. This story is told in *SHARING THE SECRETS: Open Source Intelligence and the War on Drugs*.

#### 5007. Technical Intelligence

At the technical level, military lethality (including accuracy), geographic atmosphere, and civil infrastructure are important determinants of battlefield success.

As was discovered during the Gulf War, open sources are the best and often the only source of information needed to "map" the target area's C4I infrastructure, and develop information warfare operations.

Open sources are also the backbone for planning logistics operations and mobility systems, since information about airheads, ports, rail and road networks, and related support systems are all a matter of public record. There is however, an aspect of the open source world that is not obvious at first: much of what is counted as "open" source is in fact grey literature, limited edition literature in a foreign language. Collecting and processing open source information is not necessarily easy!

Finally, open sources are the foundation for long-term intelligence efforts against scientific and weapons research. Unclassified civilian research, and publications by civilians employed in defense-related industries, have long been a critical foundation for intelligence in support of major acquisition programs. In fact, one tip-off for intelligence analysts is the

disappearance from a literature of a particular expert, or a particular line of inquiry.

#### **5008. Commercial Imagery for 1:50,000 Maps**

A ten meter image from SPOT Image Corporation can be processed to integrate both the standard military grid lines, and the contour lines that most people do not realize is achievable from SPOT panchromatic coverage.

It is especially important for analysts to understand that this commercial system has been in operation for over a decade, and that virtually the entire world has been imaged, with most images being less than five years old and in ground station archives--this imagery is available within 24 hours.

Source imagery is not enough by itself, as was mentioned earlier. Additional processing is required to establish elevation points and precision points, and additional time is needed to produce the 1:50,000 combat charts necessary for combined arms operations and especially infantry patrolling....but the source imagery, traditionally the stumbling block when attempting to use national systems to obtain wide area coverage in a crisis, is no longer the obstacle to producing maps.

By combining SPOT wide area coverage with NRO precision points, under the management of the Defense Mapping Agency, we can have 1:50,000 maps right now.

#### **5009. Commercial Imagery for Mission Rehearsal**

The same commercial imagery that is used to produce 1:50,000 combat charts can also produce superb three-dimensional simulations and perspectives that can be used to study beach approaches, potential landing zones, and nape of the earth flight corridors.

#### **5010. Order of Battle Information**

The former Soviet Union and the People's Republic of China are probably the only two countries where the U.S. intelligence community could state with certainty that it possessed more accurate information about the order of battle than was available from open sources. Perhaps this is even true of other denied areas such as North Korea and Cuba.

Yet when it comes to virtually any other country, the information collected and processed by Jane's Information Group, publisher of the Jane's series of books and CD-ROMS which cover all types of mobility and weapons systems, is the world standard. In fact, in a graduate thesis by (then) Major Robert M. Simmons, titled "Open Source Intelligence: An Examination of Its Exploitation in the Defense Intelligence Community", our own military intelligence analysts are quoted as saying "reference publications such as Jane's often provide first indications of weapons modifications and sales" (page 112).

The Jane's series of references books and CD-ROMS is now also available online by special subscription, and the material is kept current by a global network of overt human assets as well as extraordinarily good relations between Jane's and most Ministries of Defense. Analysts need to know that as good as the Jane's publications are, only 20% of the information known to Jane's is actually made public. "Confidential" reports on training, morale, and other issues can be obtained by special arrangement.

Jane's is also helpful in understanding the order of battle for non-traditional information. Jane's has provided orders of battle for the warring clans in Somalia, and is considering providing a similar service with respect to transnational criminal organizations.

Another private sector service that can be helpful to analysts attempting to understand Third World or non-traditional orders of battle (e.g. of revolutionary groups) is offered by Rapport Research & Analysis, representative of a small number of elite organizations, most with Special Air Service or similar backgrounds, who specialize in making available highly trained interrogator-translators who are able to canvass refugee and exile communities to identify sources and then systematically develop the needed information as well as leads to in-country sources of potential value.

#### **5011. Historical and Estimative Analysis**

In the age of distributed information, the concept of "central intelligence" is difficult to implement, and even unnecessary. While a central coordinating authority, and bodies of trained analysts with clearances, are both needed, there is now a very robust "virtual intelligence community" which can be harnessed to develop significant amounts of historical and estimative analysis based solely on open sources.

Oxford Analytica, a U.S. owned company based in Oxford, England, is the best private intelligence agency in the world, and its excellence is based strictly on analysis. Founded by Mr. David Young, who worked with Dr. Henry Kissinger when the latter was National Security Advisor to the President, Oxford Analytica specializes in producing daily regional reports which concisely address three questions: what's right in the news that needs elaboration? what's wrong in the news that needs correction? and what weak signals are we seeing that merit scrutiny and an estimate?

This organization covers the world. For Somalia, to take one example, over a period of two years they produced over twenty two page reports on UN operations in Somalia, US foreign policy toward Somalia, and US operations in Somalia.

How does this "best in class" organization work? They start by having a fifteen person team, organized by region and function, review all news wires and major periodicals on a day to day basis. They then bring in the Dons of Oxford in small groups rotated regularly, and draw on the expertise resident at Oxford University—in effect they have harnessed the centuries of accumulated experience, and integrated that experience into their

daily operations. Then, when special reports are desired, they have a global network of 1,000 experts, culled down from 2,500, to whom they can turn at any time with a request for a two-page report which integrates personal calls to key decision-makers, and is drafted at a level suitable for a President, Prime Minister....or you, the analyst preparing intelligence products for policy-makers and commanders.

## 5012. Networks of Experts

The most significant difference between elementary and advanced analysis is that the first draws primarily on published information, and the second draws primarily on direct contact with world class experts.

Most published information is out of date by the time it is published. In addition, the intelligence community, which specializes in secrets, is not trained, equipped, and organized to collect open source materials. The result, well documented in the thesis by Major Simmons cited earlier, is that analysts have very limited access to the broad capabilities in the private sector. Advanced analysis requires recourse to a network of expert colleagues in the private sector who can serve as a collection filter, and quickly identify key documents, comment authoritatively on emerging trends, and generally help the advanced analyst to fully exploit open sources, while also adding the unique value that is inherent in all-source analysis.

LEXIS-NEXIS and DIALOG, the two major online news services, are recommended to analysts not for the massive volume of printed information they can provide, but for something far more subtle: the identification of journalists and sources who—through their by-lines or their being cited, might aid the analyst in leap-frogging over old published information and into the future.

Complementing the online services is the Institute of Scientific Information, and its two major publications, the *Social Science Citation Index* and the *Science Citation Index*. These are unique databases, available both in hardcopy and online, because they allow the analyst to take an older work known to be relevant, and to quickly identify, right up to the current week, who has cited the older work. In essence, the analyst can quickly reach the most current and authoritative experts on any topic through this capability, with the added advantage that frequency of citation conveys a sense of peer evaluation.

Professional associations and associations of retired military personnel are mentioned simply to highlight the fact that the entire world is full of knowledgeable people, most of whom would be happy to respond to questions. Finding the right person and asking the right question is becoming more important than "keeping up with traffic".

### 5013. Expeditionary Factors Study

The *Expeditionary Factors* study sponsored by the Marine Corps Intelligence Activity and carried out by PRC under contract, is a second generation effort, and current as of 1994. It is a showcase for OSINT, as it is the only high-level intelligence community product that relies exclusively on open sources, and is published in an unclassified form (For Official Use Only).

The first generation study was completed in 1990, and was called *Overview of Planning and Programming Factors for Expeditionary Operations in the Third World*. Copies of the original analysis model, and of the strategic generalizations chapter from the original study (this chapter was inadvertently overlooked in the follow-on study and thus was not updated), are included as hand-outs.

The other unique aspect of the Marine Corps study was its focus on countries which the Marine Corps felt has the "highest probability" of requiring entry by U.S. forces, rather than on the traditional "worst case" priorities focus. The original list of countries, approved by the Marine Corps flag officer community, was comprised of 69 countries. The current list includes 80 countries, almost all of them in the Third World.

The Marine Corps approach, besides focusing on open sources and an unclassified product, was also unique in that warfighters--operators--were asked to define low, medium, and high degrees of difficulty for each mission area, and this was then converted into a five point scale that can be graphically depicted.

This three-volume hard-copy set, also available on CD-ROM, is an excellent ready reference for planning, and is available. To obtain ordering information, call or fax the numbers shown here.

### 5014. Strategic Generalizations

Having introduced the *Expeditionary Factors* study, we now turn to some of the strategic generalizations which emerged from its predecessor and remain constant today.

The expeditionary environment is complex and lethal. Experienced infantry, modern armor, sophisticated artillery, night/all weather aviation, and integrated air defense systems are all too often characteristic of the "Third World".

The "cultural terrain" is steep, with 40 of the original 69 countries speaking Arabic or a primary language other than English, French, or Spanish, and most practicing Islam or an eastern or trivial religion.

The aviation temperature is uniformly hot, with a sustained heat index of over 80 degrees, which automatically reduces both lift and range of aviation platforms significantly.

There is an equal mix of mountains, deserts, jungle, and urban terrain. We must be ready for all four. Cross-country mobility was non-existent in 60% of the countries and severely constrained in another 20%. When combined with an average bridge loading capability of no more than 30 tons (not in the study but well-known as the civilian limit for truck weight), this suggests real difficulty for existing concepts of ground maneuver.

Average line of sight distance was under 1,000 meters, with only eight of the 69 countries offering stand-off engagement ranges of over 2,000 meters. In the absence of carrier aviation, the Navy's standard guns are no match for the coastal artillery and missiles of many of these countries.

There were no 1:50,000 maps for 22 of the countries, and old maps for ports and capital cities only of another 37 of the countries.

Finally, between half the countries having no usable ports, and most capital cities with their Embassies being beyond the round-trip range of a CH-46 flying from the five fathom line, Non-Combatant Evacuation Operations presented real challenges.

#### **5015. Commission on Intelligence**

Open sources are gradually being accepted as an important part of the all-source production process, but there are still many obstacles to its full integration into national and defense intelligence.

The Commission on Intelligence, popularly known as the Aspin or Brown Commission, was created by Congress to thoroughly evaluate the U.S. intelligence community. One of the closed hearings held by the Commission, on 3 August 1996, addressed open sources. Among the four individuals testifying were the National Security Advisor to the President, Dr. Anthony Lake and the founder of OPEN SOURCE SOLUTIONS, Inc., Mr. Robert Steele.

At the end of the session, a Thursday afternoon, General Lew Allen, USAF (Ret), challenged Mr. Steele to join in a benchmark exercise testing private sector capabilities against those of the entire Intelligence Community. Burundi was chosen as the target, and a deadline was set for 1000 the following Monday.

The Commission was surprised by the results. In short order, they received order of battle information on tribes from Jane's Information Group; strategic commentary from Oxford Analytica; a list of available Russian maps down to the 1:250,000 level from Eastview Publications; a list of authoritative journalists from LEXIS-NEXIS; and a list of expert academics and others from the Institute of Scientific Information. Later, not part of the initial response, it was determined that SPOT imagery was available for all of Burundi and could be used to produce 1:50,000 combat charts and mission simulation programs.

As a direct result of this benchmark exercise, the Commission included in its final report an extraordinarily detailed and strong statement on the importance of open sources. The Commission noted that OSINT has limitations, but went on to state that the Intelligence Community has been "inexplicably slow" to provide analysts with access to open sources; that the Commission views such access as "critical" to the all-source analysis process; and that the Commission believes that open source access should be a top priority for the Director of Central Intelligence and a top priority for funding.

## **5016. Conclusion**

Commercial imagery is a useful example of how open sources can support and enhance national intelligence capabilities:

- 10 meter commercial imagery provides cheap and fast wide-area coverage, and has the added advantage that most of the world has already been overflowed and generally cloud-free imagery are already stored in the ground stations;

- 1 meter commercial imagery--if U.S. policy and a lack of funding does not derail private sector efforts to create this new capability--can provide urban detail and a closer focus on key targets while avoiding an order of magnitude increase in the cost of maps which would accompany any attempt to use 1 meter for the whole world (not to mention the delay in collection); and finally

- Classified imagery from the National Reconnaissance Office can provide the eight precision points per wide-area image that are necessary to create a 1:50,000 map to our standards of accuracy for combined arms operation.

The Defense Mapping Agency, or the new National Imagery and Mapping Agency, are ideally placed to manage a truly national program in which private sector open sources and classified Intelligence Community capabilities are fully integrated. This is the ultimate value of open source intelligence--as an integral part of the all-source solution.

What should we conclude from all this? First, it is clear that experts and data reside in the private sector, outside the intelligence community, which are vital to understanding and which should be harnessed in support of the all-source intelligence process. Second, these resources represent a potential source of savings to the U.S. taxpayer, since they are maintained at no cost to the taxpayer, are constantly validated by their survival in the marketplace, and--if properly exploited--permit the expensive classified capabilities to be applied more effectively to "the hard stuff". Open sources provide orientation and context. They do not provide the complete answer in most cases, but rather make the other intelligence disciplines more effective.

## **Chapter 6**

### **OPEN SOURCES AND OPERATIONAL SECURITY--THE DARK SIDE**

#### **6001. Purpose of the Chapter**

This chapter was developed by Mr. Richard Horowitz, a licensed private investigator and security consultant based in New York. Mr. Horowitz has served in the Israel Defense Forces, attaining the rank of Captain, and is now studying law in New York City.

This chapter is grounded on the premise that everything needed for the planning and execution of criminal or terrorist activity can be found in open sources. Indeed, an entire industry exists which is devoted to the publication of such material. In addition, equipment designed for one purpose and legally available can be used in terrorist or criminal activity.

The total cost of the publications and equipment presented in this "dark side" chapter is available for approximately \$1,800. The chapter is based on the "seeing is believing" principle. Each of the items discussed in this chapter can be ordered by using the complete ordering information containing in Appendix G.

From both a military and a law enforcement point of view, it is critical to understand that even our most poorly-funded and least organized opponents can gain access to relatively sophisticated intelligence collection tools as well as tools of destruction.

This chapter--like all other chapters in this handbook--is unclassified. The key point to emphasize is that everything presented is publicly and legally available. Books on intelligence collection, killing methods, offshore money laundering, and any other aspect of criminal operations can be purchased by calling an (800) number and using a credit card. We must all be aware of how such information might be exploited when acquired by persons seeking to harm or take advantage of others, and specifically, to harm members of the MAGTF in garrison or ashore.

#### **6002. General Considerations**

It is a fact of life that society contains those who are morally deviant, socially misguided, or worse. It is of similar importance that our society is based on certain freedoms which cannot be taken away. The combination of the two can result in terrorism and crime as we know it today. Underlying the activities of these individuals and groups is a culture which includes recruitment, indoctrination, education, training, planning, preparation, and execution.

This chapter is not a training manual, though many techniques and methods can be recognized from professional government training. The objective is to create an awareness regarding the availability of open sources for terrorist and criminal activity.



Four general considerations are offered as an introduction to this model:

1) The availability of the open sources to criminals and terrorists, and the extent to which such capabilities exist, does not document a threat *per se*. Each individual command and each individual operation must carry out a threat analysis unique to their circumstances.

2) Everything we discuss in this chapter is available to anybody anywhere. This includes Colombian drug smugglers, Los Angeles gang members, Korean contract employees on a U.S. Army base overseas, and individual "crazies" seeking media attention by causing deaths or damage aboard U.S. military installations.

3) Information that has been available for years in published form is now available through the Internet. Bomb designs are popular in cyberspace. Periodic press reports tell of teenagers injuring themselves trying to construct a bomb they have read about on the Internet. While this problem will arguably increase, it should not obfuscate the reality that the industry which produces the material in hard copy has existed for many years.

4) Although "high-tech" threats attract more media attention, the reality is that low-tech capabilities are often just as effective, cheaper, and easier to develop. A federal officer can be attacked by a doberman with its vocal cords cut out—a low-tech but very effective means of perimeter security. The bomb used to destroy the Federal Building in Oklahoma City was not a complex construction—it was a simple mix in a large amount.

#### 6003. Open Sources and Radio Interception

Intelligence acquisition, or information gathering, is a crucial first step in planning and executing an operation. The next six slides are devoted to various methods of information gathering: electronic monitoring, operational activity, and computer databases.

This split slide shows frequencies for Air Force One on the left, taken from a book by a California hobbyist which is devoted to monitoring the President. Entitled "Monitoring Air Force One," the volume discusses and lists frequencies of the Mystic Star, Echo/Foxtrot, and FM-FDM-SSB systems, along with identified Secret Service code names.

On the right is the cover of a book published in 1986, entitled *Guide to Embassy and Espionage Communications*, which listed thousands of frequencies transmitted from 55 countries, the International Red Cross, Interpol, and the United Nations.

The extent to which frequencies of federal and state agencies that are intercepted and published presents a security problem is not within the scope of this chapter. The range of equipment and information commercially available indicates a problematic potential or at the very least, can be an incentive for subversive groups to attempt to intercept government transmissions.

Commercially available radio scanners can intercept UHF, VHF, and military bands; some have uninterrupted frequency ranges from 30 MHz to 1.2 GHz and are available in desk top or portable versions. Current law requires manufacturers to block cellular telephone frequencies.

Frequency counters-devices that intercept radio transmissions and display their frequencies on a read-out-are also commercially available.

*Monitoring Times* runs a column which publishes frequencies used by federal agencies that were intercepted by hobbyists. These agencies include the F.B.I., Secret Service, U.S. Customs, and numerous military agencies. After the World Trade Center bombing, the magazine carried an article listing frequencies used by various Port Authority units, the FAA, and local "press disaster" frequencies. Guides to U.S. and allied official frequencies are readily available worldwide--if a hobbyist can track you, so can a criminal!

#### **6004. Open Sources and Telephone Interception**

It is illegal to monitor cellular phone conversations (868-896 MHz). Prior to April 1994 however, radio scanners capable of intercepting these frequencies were legally manufactured and sold. Scanners that blocked cellular frequencies were constructed such that they could be easily modified to intercept cellular transmissions.

Scanners manufactured before April 1994 can still be legally owned or sold. Hence, many scanners capable of intercepting cellular calls are accessible and in use.

Some methods of scanner modification:

- A Massachusetts company advertises that for \$40, they will "unlock" your scanner
- Journals print schematic diagrams showing how to modify the scanner's circuitry;
- While the new law prohibits the manufacture of frequency converters- a device that will convert 400 MHz interceptions to 800 Mhz interceptions, many are accessible.
- For those with technical skills- a cellular phone, which needless to say operates on cellular frequencies, can be modified to intercept other cellular calls.

A book entitled *Tune In On Telephone Calls*, listed in your second hand-out, enumerates frequencies and channels used in various types of telephonic transmissions. Its various chapters cover such operational relevant areas as military aircraft VIP phone calls, satellite phone calls, coastal maritime calls, and cellular calls.

In addition to voice and data interception, there is a commercially available device called a tone decoder which converts the frequencies of a touch-tone dialing system to

numbers and displays them on a read-out, in effect allowing easy identification of those being called by the intercepted telephone, as well as read-out of any other information being transmitted through the touch-tone signals, such as codes and account numbers.

Internationally, for instance from Switzerland, more sophisticated equipment is available, and we should assume that surplus or illicitly obtained military equipment is also available to individuals to whom good intercepts are critically important.

#### **6005. Open Sources and Eavesdropping**

Numerous books are in print detailing how to tap a phone or bug a room. Some are quite technical. A manual originally published by the U.S. Department of Justice entitled *Electronic Eavesdropping Techniques and Equipment* has been republished under a different title by a commercial publisher, and is listed in your second hand-out. Please note that "old" techniques can be very effective, especially if there is very little emphasis on operational security against civilian opponents!

In April, 1995, U.S. customs officials raided 40 spy shops in 24 cities that were illegally selling eavesdropping equipment smuggled into the United States from two Japanese companies; 11 people were charged with crimes as a result. Termed "electronic surreptitious interception device," among the equipment smuggled into the United States and sold by these shops:

- telephone transmitters with a range of 400 meters
- bugging transmitters with a range of 1,000 meters
- ball-point pen transmitters with a range of 200 meters
- A/C line transmitters-attached to the line, behind the wall outlet and permanently operates on its current-with a range of 200 meters.

From documents filed in court by the U.S. Government, from October 1993 through February 1995 a total of 161 shipments of 4,367 eavesdropping devices took place. The devices had an estimated retail value of \$2,972,517.

Companies also publish electronic plans enabling an individual to assemble his own equipment. These schematic diagrams include automobile tracking transmitters, bugging transmitters, telephone transmitters, a transmitter locator, and audio amplifiers.

Bottom line: assume you are "on the air" unless certain the circumstances are secure!

## **6006. Open Sources and Undercover Operations**

Undercover operations is a term used to describe various types of activities designed so that the fact they are taking place is not recognized, or, if recognized, not for what it really is. The general purpose of undercover operations is generally either to affect a change on a target or to gather information about a target.

Manuals for private investigators, as well as training manuals for law enforcement from various countries have made virtually all aspects of undercover operations a matter of public record. There are manuals on undercover operations in general, on developing clandestine human networks, on surveillance, on lockpicking, and even on elicitation and pretext calls, a very common technique for obtaining information.

Books are in print containing prepared scripts for obtaining personal and financial information from people. One book opens with a chapter entitled "Establishing Rapport and Overcoming Objections." Complete citations are in your second hand-out.

This slide shows two illustrations, one from a manual on surveillance techniques, the other from a manual on lockpicking. Complete citations for both are listed in your second hand-out.

Lockpicking tools are legally sold; prices can start from about \$25. The law does not criminalize possession of lockpicking tools unless the person possessing the tools "evinces an intent" to use them for burglary. To quote the New York State law:

"A person is guilty of possession of burglar's tools when he possesses any tool, instrument, or other article adapted, designed or commonly used for committing or facilitating offenses involving forcible entry into premises...under circumstances evincing an intent to use or knowledge that some person intends to use the same in the commission of an offense of such character."

It merits comment that with the limited number of known aerial and maritime surveillance platforms that the U.S. Coast Guard has to patrol the drug routes from Latin America to the United States, it would be an easy matter for drug criminals to establish both passive observation posts near airfields and ports, and also active aerial and maritime surveillance capabilities. In brief then, criminals and terrorists who understand the value of intelligence collection, can easily establish significant capabilities which can frustrate official government programs.

## **6007. Open Sources and Interrogations**

Criminals and terrorists have access to professional training and professional interrogators. Even the most reputable firms, such as E2G and Rapport Research in the United Kingdom, both staffed by highly trained former Special Air Service (SAS)

interrogator-translators, will be happy to offer training and perhaps even surveillance and other services to those who come to them with cash and an appropriate cover story.

In the United States, the "Soldier of Fortune" circuit includes many training and exercise schools where useful knowledge can be learned.

This slide listed selected chapter headings from two books readily available on the open market, one on psychological interrogation techniques, the other on physical interrogation techniques.

As transnational crime becomes a greater threat to national security, and the military become more involved in support to law enforcement operations, it merits comment that operational security and "need to know" are just as important in this environment as in any other.

Indeed, one of the distinguishing aspects of transnational criminal operations are their ruthlessness, and the ease with which they can select and coerce civilians to help them on a one-time basis by threatening to kill their loved ones—how many Pacific Coast fisherman do you suppose would refuse to carry one load of drugs if they were assured that it would only be a one-time risk, and that their loved ones were being held under surveillance and would be killed if the fisherman did not cooperate?

#### **6008. Open Sources and Direct Research**

Previous chapters have dealt with the rich range of open sources, and how to develop intelligence from open sources, including international sources and the Internet. The point to emphasize is that terrorists and criminals have access to everything in the open source world described by this handbook.

Major criminal and terrorist organizations are fully cognizant of the utility of open sources, and know how to do their homework. They know the power of computerized search & retrieval, and the value of information in support of their operational objectives.

For the purposes we are discussing, the computerized databases which can be accessed by anyone in the public, including criminals and terrorists, can be divided into the following three broad categories:

— Media: available are not only *The New York Times*, *Washington Post*, and *Wall Street Journal*, but numerous local newspapers such as *The Rocky Mountain News* (Denver, CO), *The Commercial Appeal* (Memphis, TN), and *The Times-Picayune* (New Orleans, LA), and foreign newspapers such as *Le Monde*, *The Irish Times*, and *The Prague Post*. Wire services—UPI, AP, Reuters, and the Xinhua News Agency (China), for example, are also accessible.

-- Business and public records: corporate and bankruptcy filings, SEC filings. property ownership, criminal background checks, driver's licenses. Financial news. Companies combine mailing lists of hundreds of marketing companies, resulting in a database which can identify the address of a person or family, or their neighbors. Reverse phone directory-enter name, retrieve a person's phone number, or enter a phone number and retrieve the name of the person.

-- Specialized trade and industry information: databases exist that specialize in information unique to a particular industry or country, generally in the form of periodic newsletters, and are a valuable source of information. This slide lists some of the sources of possible use to criminals planning electronic thefts or money laundering operations, and terrorists planning specific acts.

A classic example of the basic utility of research: on 3 May 1993 a complete report was carried online about the meeting of the Nuclear Regulatory Commission, entitled: "Commission Hears Options for Dealing with Vehicle Bomb Threats". Discussed in detail online: the four options regarding physical barriers surrounding nuclear power plants.

#### **6009. Open Sources and Executions**

This slide is a combination of extracts from two books, one on killing and one on creating silencers.

Literature on killings and executions are graphic and the methods described are real. A six volume work entitled "How To Kill" is representative. Volume One begins with "Chapter One: The Target," complete with an anatomy chart highlighting sensitive parts of the body. Subsequent chapters are devoted to various types of killings. Appendices entitled "The Signs of Death," "Your First," and "A List of Poisons" follow the chapters.

A separate body of literature exists on the use of knives. One book has the topical heading of "anatomical considerations" followed by diagrams entitled bleeders, immobilizers, quick kill, showing the respective spots on the body. The book ends with an appendix entitled "Suggestions for Further Study."

Books describing how to construct silencers from household material exist. Attaching a slightly filled plastic soda bottle or a container of three tennis balls to the barrel of a gun are crude methods. More technical methods requiring metals are detailed. In a chapter entitled "Your Last Chance To Be Legal," one book discusses the various federal forms that need be filed in order to request to manufacture a silencer.

Manuals on improvised weapons show how to install a gun or firing mechanism in, for example, an umbrella, belt buckle, flashlight, briefcase, cigarette lighter, or tobacco pipe.

The same publisher selling books on how to kill supplies a book on how to dispose of dead bodies, including a technique on removing a bullet from a body without leaving evidence.

Full citations to all the books cited in this chapter are contained in Appendix G.

#### **6010. Open Sources and Explosives**

This slide is also a combination of several diagrams to illustrate the nature of the information that is available in open sources about creating and using explosives.

Improvised explosives, and bomb design, are topics with the most published literature. Numerous books in a "cook book" form describe how to mix readily available chemicals into explosives. Mixing soap flakes with gasoline so as to allow the gasoline to stick to its target instead of dripping off before igniting is discussed in a book and in a video on making explosives.

Separate books exist on how to make C4 and Semtex.

While these books generally have a disclaimer that the information contained therein is for educational purposes only, a book entitled "Professional Standards for Preparing, Handling, and Using Explosives" is available from the publisher.

From a catalogue:

**DEATHTRAP! The Video:** There is no better way to learn about improvised explosive booby traps used by international terrorists than to watch live, on-camera demonstrations of their construction, deployment and detonation. **DEATHTRAP! The Video** is a chilling seminar in just that - how terrorists modify innocent everyday items to conceal insidious explosive booby traps designed for maximum shock and lethality. You'll see ingeniously disguised devices made out of books, music cassettes, mugs, portable tape players, foot powder cans, alarm clocks, videocassettes, mousetraps, and more, all triggered by simple electrical, chemical, or mechanical means.

The video costs \$29.95 and runs for 35 minutes.

A wide variety of related books are also available, for instance on bridge demolition.

#### **6011. Open Sources and Radio Detonation of Bombs**

Apart from simple explosives, it merits comment that sophisticated devices for detonating explosives from a distance are readily available to criminals and terrorists.

Bombs can be detonated by remote control, through radio detonation. The chip needed for production of the detonating tone retails under \$20.00.

A book entitled *Improvised Radio Detonation Techniques* describes how to modify various types of radio equipment into detonation transmitters. This slide lists devices afforded a chapter in the book, along with relevant information regarding their modification.

In March, 1994, this book was among numerous other books found in a storage locker of a man suspected in the package bomb that killed five people in upstate New York. In a similar incident, on February 10, 1995, the Associated Press released a report of a high school student's locker booby-trapped with a set of firecrackers wired to a circuit board and capable of being detonated by radio control.

Radio detonation, including that of car bombs, is a major problem worldwide:

- In May 1992, the Mafia killed Judge Giovanni Falcone and three bodyguards with a car bomb detonated by remote control while they were driving along a Sicilian highway.

- A March 1994 article in the Current Digest of the Soviet Press entitled "Who's Getting Killed In Moscow, and How" cited the problem of remote control detonation.

- In January 1995, a group that manufactured radio detonated bombs was arrested in St. Petersburg. Constructed for \$60 and sold for \$1,500, the bombs came with a six month guarantee.

According to the Intelligence Newsletter of March 16, 1995, Egypt spent \$18 million in 1994 on equipment to detect car bombs and to jam their detonation frequencies.

## **6012. Open Sources and Vehicular Enhancements**

Evasion is a significant concern after executing an operation. There are a number of enhancements that can be made to vehicles, enhancements which can increase chances of evasion if detected and pursued. Some possible enhancements are listed in this slide.

There is a thriving small industry specializing in the production of armored cars for civilians. Publications such as *The ROBB Report* routinely advertise all manner of armored vehicles for sale--vehicles which to all outward appearances, are simply a normal car.

In addition to enhancements to the individual vehicle, skill at evasive driving is crucial in case operatives are detected. One manual on evasive driving illustrates evasive techniques on city or country roads, and in chase situations, along with automobile security modifications such as an oil slick or smoke screen generator. In case the driver does not successfully evade the pursuer, techniques for knocking the pursuer off the road are described. The manual has a chapter entitled "Suggested Training Schedule."



This is a good point in the chapter to emphasize that criminals and terrorists are very aware of the fact that they pursue very high-risk, high-gain occupations, and have a great deal to gain from proper preparation. Their preparations are all the more difficult to deal with because by definition they are camouflaged as civilians and do not wear uniforms or follow any recognized rules of engagement. Establishing their technical capabilities and their "order of battle" thus calls for entirely different collection methodologies.

### **6013. Open Sources and Tactical Communications Jamming**

Military forces rely heavily on command & control, and on combined arms operations. Military patrols in support of law enforcement operations are relying on artillery and other forms of reinforcement as they venture out "on point". It therefore becomes important to understand that criminals and terrorists are capable of executing tactical communications jamming operations.

Although radio jamming is illegal, *Improvised Radio Jamming Techniques* is a technical book describing the construction of a jamming station, allowing an operative to jam radio transmissions of government agencies as part of an operation or during the evasion stages.

Chapters in the book include:

- Intercept Equipment Selection
- Covert Antenna Systems
- Intercept Operations
- Police Radio Operational Procedures
- High-Risk Frequency Detection Techniques
- Jamming Equipment Deployment
- Operational Security

### **6014. Open Sources and Bank Card Forgery**

Central to criminal and terrorist operational security is the creation of a new identity, or a variety of identities that frustrate the efforts of law enforcement officials to track their international and domestic movements. The methods of creating a new identity in various books range from obtaining a new public image to physically disappearing and altering one's identity. Some books on creating a new identity focus on obtaining public records under a new name. Chapters are devoted to social security cards, driver's license, credit cards, and bank statements.

Other books exist on how to produce counterfeit identification documents. One book contains chapters such as *The Forger's Kit*, *Forgery Techniques*, and *Quality Control*, and discusses the "False Identification Crime Control Act of 1982" which prohibits selling fake I.D. by mail. The book continues: "It's still possible for the forger to buy the various

materials needed to produce fake I.D." and provides names and address and several companies.

A separate book exists devoted to counterfeiting currency. Chapters include "Basic Printing Techniques Used in Counterfeiting," "Purchasing Equipment and Supplies," and "Passing Counterfeit Currency."

Worldwide contacts, and world-wide mail drops, are readily available to criminals and terrorists. Companies publish booklets listing lawyers, bankers, and accountants in numerous countries ready to take a call from someone in need, together with lists of thousands of companies providing voice, fax, and correspondence forwarding services.

These are the traditional methods. Today, "cyber-theft", and direct anonymous access to bank accounts, as well as the complete concealment of international financial transactions through encryption and anonymous remailers, is becoming the major foundation for global criminal activity. One good reference is *Electronic Fund Transfer Systems Fraud*, published by Paladin Press (ISBN 0-87364-490-5).

#### **6015. Open Sources and "Legal" Offshore Passports**

Companies will, for a fee, arrange a legal passport and citizenship for their client, from a country not the person's country of birth.

Below is the fee scale from a company based in Amsterdam which specializes in passports and citizenship from Latin American and Caribbean countries--a legal citizenship which can be obtained within 90 days of submitting the company's application.

Dominican Republic	\$19,500 for 1-4 individual orders
Venezuela	\$21,900 for 1-4 individual orders
Panama	\$20,900 for 1-4 individual orders
Ecuador	\$23,900 for 1-4 individual orders

The application requests information such as the applicant's name, date and country of birth, height, eye color, visible scars, existing citizenship, profession, and mother's maiden name.

Along with the application, one need submit:

- the signature and photo page of the applicant's current passport
- copy of a birth certificate
- three color negatives in three different sets of clothing
- affidavit of good conduct from a licensed attorney or local police clearance
- six thumbprints
- six signatures on a white sheet of paper

-- a personal character reference or bank reference

The company's material explains that one need not visit his new country but can remain a "citizen living abroad," and contains a chart indicating countries that can be entered without a visa with your new passport.

The company can arrange a diplomatic passports "to some," for a fee of \$55,000.

A midwest American company offers "genuine" passports and driver's licenses from countries that no longer exist, such as Burma, Rhodesia, Dutch Guiana, and the Republic of Zanzibar. The company portrays these passports as "emergency passports," in case terrorists hijack a plane and the American traveller would not want to identify himself as such. The application requires only a name and credit card number.

A U.S. Government "Passport Agent's Manual" has been acquired and republished by a commercial publisher. The manual is a useful guide for avoiding obvious mistakes.

#### **6016. Open Sources and Offshore Corporations**

In addition to arranging second passports and citizenship, companies exist that will establish shell companies for their client, generally offshore.

One British company specializes in establishing companies in the Bahamas, Belize, the British Virgin Islands, Delaware, Gibraltar, and Panama. The company's promotional material contains a chapter on each country, reviewing the requirements regarding:

- capital and shares
- directors and shareholders
- meetings
- accounting
- corporate seals
- company name
- registered agent, office, and domicile

The application form requests only the name of the company to be established, the names and nationalities of the shareholders and directors, the objective of the company, and the applicant's name and address.

A Hong Kong company will also form a company in numerous localities around the world, from the Cayman Islands in the Caribbean to the Isle of Man located in the Irish Sea. The company's specialty however is Hong Kong "shelf companies"- corporations ready for purchase.

The Hong Kong company provides a list of over one hundred shelf companies incorporated in Hong Kong. Company names were chosen, apparently with the intent of attracting American buyers. These shelf companies were incorporated in 1993-94, allowing the company's purchaser to give the impression that the company had been in business years before the purchaser took control.

The application form requests only the names, business occupations, nationalities, and passport numbers of the company's officers and directors, along with information on the purchaser's bank account. For the client's benefit, the Hong Kong company includes educational material on how to arrange letters of credit through the client's new offshore company.

#### **6017. Open Sources and Choosing a Criminal Specialty**

Similar to books on individual methods and techniques, books are available on crime as a profession. For example, a book entitled *Drug Smuggling* contains information on how to find a drug source, what type of airplane is suitable for smuggling, and how to launder money. It closes with a discussion on dealing with law enforcement and a chart detailing federal and state drug laws, shown in this slide.

A book entitled *Successful Armed Robbery* written by an inmate in a federal penitentiary, contains the following chapter headings:

- The Selection Process
- Strategic Production-Planning
- Factors Affecting Your Success
- Self-Caused Failure

This book contains diagrams of various types of parking lots and illustrations on how to approach and assault the driver of a car.

*Hit Man; A Technical Manual for Independent Contractors* covers the entire range of activity for the planning and execution of a contract murder. Topics range from surveilling the target to psychological approaches to the job. From a chapter entitled "Finding Employment, What To Charge, Who To Avoid": "Prices vary according to risk involved, social or political prominence of the victim, difficulty of the assignment, and other factors. A federal judge recently brought the price of \$250,000, according to one example provided. A county sheriff might bring \$75,000 to \$100,000."

A related book entitled *How To Hide Anything* is available to criminals and terrorists. It contains numerous diagrams illustrating the construction of hiding compartments for objects or people in indoor and outdoor settings, and can be used to create hiding places for contraband, documentation of illegal exchanges, and special illegal technical equipment.

The list goes on. There is a market in information about how to be a criminal or terrorist, and there are established concepts, doctrines, and information about organization, methods, and equipment which is readily available world-wide.

#### **6018. Conclusion: The Dark Side of Open Sources**

This chapter has reviewed the open source knowledge available to criminals and terrorists which, when properly utilized, can make the military mission and the mission of law enforcement more difficult.

In particular, this chapter has sought to emphasize that operational security and the "need to know" are important aspects of success against a well-trained and well-equipped criminal or terrorist organization which understands the value of intelligence collection.

Criminals and terrorists can intercept radio and telephone conversations; they can exploit eavesdropping devices and execute tactical signal intelligence collection operations. They know how to conduct undercover operations, how to interrogate captured prisoners, and how to do direct research using open sources.

Individuals can be effective at executions and in the use of explosives. Radio detonation of explosives through a variety of remote devices is easily understood and readily carried out.

In the escape and evasion phase, criminals and terrorists can exploit armored vehicles equipped with oil slick and other devices for delaying pursuit, and can also execute tactical jamming operations which may allow them cut off and surround their military or law enforcement pursuer before back-up forces can be mobilized.

In conducting transnational criminal and terrorist activities, these individuals can avail themselves of false credit cards, new identities including legal passports possibly obtained through false supporting documentation, and related corporate and letter of credit documentation.

Over all, this chapter has sought to communicate the degree to which information about various criminal professions is available in the open source world, allowing for knowledge about how to conduct many different kinds of crimes and illegal activities to pass from one generation of criminals to another.

Criminals and terrorists can think and read--open sources are as useful to them as they are to intelligence professionals and the operational commanders they support.

## **Chapter 7**

### **CONCLUSION: COLLECTING AND PROCESSING OPEN SOURCE**

#### **7001. Purpose of the Chapter**

This final chapter wraps up the handbook by providing information about three official U.S. government channels for obtaining open source intelligence: the Community Open Source Program Office and its global Open Source Information System; the Defense Intelligence Agency Open Source Program and the (planned) Defense Intelligence Agency Open Source Intelligence Center; and--especially important for Marines--the Marine Corps Intelligence Activity and the Expeditionary Factors Study. The Chapter concludes with a brief discussion of the usefulness of the Marine Corps Reserve as a source of existing and new open source exploitation experts, and some recommendations on additional open source training opportunities.

#### **7002. Community Open Source Program Office**

The Community Open Source Program Office (COSPO) was established effective 1 March 1994 by DCID 2/12, which superseded the earlier establishment on 1 June 1992 of the Open Source Coordinator. The requirement for an Open Source Coordinator first emerged in 1992 as a result of the findings of the Open Source Task Force, one of eleven task forces that Congress required the Director of Central Intelligence to establish as part of his confirmation process. Although all elements of the Intelligence Community have used External Research & Analysis (ER&A) funds to contract for academic and technical research, and the Foreign Broadcast Information Service (FBIS) of the Central Intelligence Agency has been responsible for monitoring foreign print media as well as radio and television broadcasts, the task force concluded that a focal point would be helpful to the DCI.

According to DCID 2/12, "The COSPO is responsible for the definition and defense of the Open Source Program in the planning cycle, and for providing guidance and oversight to the program in the execution cycle. The Office, with Community departmental open source program managers, develops an optimum allocation of resources across the Community in the execution year, subject to ratification by the Open Source Steering Committee. ... the objectives of COSPO are to:

- a. Oversee a process for coordinating responsive actions to satisfy user needs.
- b. Provide advocacy and defense of departmental development and operational efforts.
- c. Ensure funds for critical open source activities.

d. Oversee a process for identifying and prioritizing open source substantive requirements."

COSPO functions include strategic planning, program formulation and representation, initiative and innovation sponsorship, operational services of common concern, systems architecture, development of services of common concern, and open source advocacy and representation.

Speaking publicly to the annual international conference on open source intelligence, in 1995 Dr. Joseph Markowitz, the Director of COSPO, stated that roughly 40% of the all-source product funded within the National Foreign Intelligence Program comes from open sources, at a cost to the program of only 1% of the total budget. Experts generally agree that the percentage of the open source contribution will vary from zero to 100 percent depending on the problem, and that an average of 40-60% is readily certifiable. Somewhat unexpectedly, open source receives great credit against terrorism and proliferation, and is said to account for as much as 80% of the all source product in those two reporting areas.

### **7003. Open Source Information System**

The Open Source Information System (OSIS) is the principal means by which COSPO is seeking to enhance analyst access to open sources. However, as it is limited at this time to information available in electronic form, it must be regarded as a very positive but only partial solution.

OSIS is an electronic network which provides both access to and sharing of unclassified U.S. Government and other open source information about Intelligence Community (IC) agencies and selected other organizations with similar information requirements.

OSIS is being installed at the various Joint Intelligence Centers, and should one day be accessible to any Marine Corps intelligence professional afloat or ashore. Examples of the information available in OSIS include:

- Jane's Electronic Library of 24 titles providing up-to-date information on military equipment, weapon systems, and defense products worldwide

- IC ROSE, a database service providing fulltext articles from hundreds of periodicals on a wide range of subjects

- FBIS products online, including the Daily Reports, S&T Perspectives, Trends, and Pacific Rim Economic Review

- Oxford Analytica Regional Daily Reports (Strategic Political and Economic Intelligence)

-- DTED, the Defense Mapping Agency's online Digital Terrain Elevation Data map collection providing worldwide coverage

-- CIRC, a database of over ten million titles on scientific and technical topics, including patents, standards, military equipment, and systems

-- a Conference Database of upcoming symposia, congresses, conventions, etcetera, in the areas of science, technology, engineering, politics, and economics

-- Unclassified library holdings of several OSIS member agencies including DIA

OSIS also offers specialized tools, such as the National Air Intelligence Center's SYSTRAN machine translation capabilities to support real time translations of non-English language information located on World Wide Web sites.

#### **7004. Defense Intelligence Agency Open Source Program**

The Program Manager for Open Source Intelligence within the Defense Intelligence Agency is Ms. Alice Cranor, whose contact information is provided here. She serves as the DIA representative to the Open Source Council, which is the advisory body formed to support the Community Open Source Program Office (COSPO). Each agency and service has a single representative to the Council. In addition to an agency-level focal point, every branch within DIA has an OSINT focal point.

Ms. Cranor, whose office code is POI-3, can be reached by voice at (202) 373-4005, via facsimile at (202) 373-8971, or via email at <AFcraat@dia.osis.gov>.

MAGTF OSINT requirements should be discussed with the appropriate DIA Branch OSINT focal point to ensure that existing DIA capabilities for accessing OSINT on that topic are not overlooked.

#### **7005. Defense Intelligence Agency Open Source Intelligence Center**

As of August 1996, a new initiative is under discussion, to create a DIA OSINT Center funded at \$10 million a year, and consisting of an EAGLE VISION ground station (to receive commercial imagery directly from commercial satellites), close to \$3 million a year to buy commercial imagery not obtainable through Defense Mapping Agency funding, and \$4 million a year to fund roughly 4,000 man-days of individual international expert support for the entire defense intelligence community. Although not yet approved, this initiative has been favorably discussed by the Director of DIA with Congressional staff, and funding is anticipated. MAGTFs should be developing their open source requirements and submitting them through appropriate channels to ensure that a fair share of these resources are devoted to expeditionary intelligence requirements.



## **7006. Marine Corps Intelligence Activity**

The Marine Corps Intelligence Activity (MCIA) has from its inception understood and valued open source intelligence. Today the primary expression of Marine Corps emphasis on the value of open source is the Expeditionary Factors Study, discussed below. In addition, MCIA has a Mapping, Charting, & Geodesy section which is able to acquire and exploit commercial imagery in support of MAGTF requirements, and all analysts are aware of the value of open sources for fulfilling expeditionary intelligence requirements.

The MCIA Librarian, Ms. Barbara Necoba, is the focal point for Marine Corps OSINT requirements.

## **7007. Expeditionary Factors Study**

In 1988, when the Marine Corps Intelligence Activity (MCIA) was first established, the first Director (a Colonel) and his civilian Special Assistant/Deputy Director discovered that much of what was needed by the Warfighting Center, the acquisition program managers, and senior staff at Headquarters Marine Corps, was not available through classified databases and classified intelligence products. In close consultation with the Fleet Marine Force, MCIA established an agreed upon list of 67 countries and two island groups against which to develop encyclopedic intelligence. Working closely with the Warfighting Center, a wide variety of mission area factors were agreed upon, and defined by the operators in terms of five levels of difficulty. Under the supervision of the Special Assistant/Deputy Director, a contractor was hired to prepare Overview of Planning and Programming Factors for Expeditionary Operations in the Third World. This three-volume product was approved by the Commanding General of the Marine Corps Combat Development Command for dissemination in March 1991, and represents the Marine Corps' ground breaking effort to create a useful intelligence product using only open sources.

Subsequently Marine Corps flag officers were consulted and agreed on a new list of 80 countries, and the study was repeated, now titled Expeditionary Force Mission Factor Intelligence Analysis Requirements Study (ExFac Study), and this new expanded study was published 15 September 1994 in both hard-copy and as a CD-ROM database. There are over 100 copies of this unique resources available throughout the Marine Corps, with one set in the library of the Navy Marine Corps Intelligence Training Center.

The following mission area factors are covered for each of 80 countries (Appendix H contains a list of the countries):

Drug Threat	Ground Order of Battle
Terrorism	Air Order of Battle
Gray Arms & Technology Transfer	Naval Order of Battle
Nuclear, Biological, & Chemical	Ongoing Conflicts
U.S. Equities	Culture

Weather  
Coastal Characteristics  
Mapping, Charting, & Geodesy  
Airfields  
Ports  
Noncombatant Evacuation Logistics  
Highways/Railways

General Geographic Conditions  
-- Cross-Country Mobility  
-- Intervisibility  
-- Operational Elevation  
Key Installations  
Communication Infrastructure  
Medical Operations

Examining the results contained in this study leads some very useful "strategic generalizations" which can help planners better prepare for expeditionary operations. For instance, the Marine Corps aviation day is hot, over 80 degrees on average, with relatively high humidity. Fewer than 50% of the ports in the this Marine Corps environment are suitable for pierside offload, requiring instream offload even when unopposed. Intervisibility (line of sight) distance in much of the Marine Corps world is heavily constrained, and cross-country mobility is almost non-existent. It should be stressed that this unclassified intelligence product is for orientation and ready reference purposes, it should not be used as the basis for planning and conducting military operations--it provides context and is intended to aid in requirements analysis and collection management of the traditional disciplines.

Every MAGTF should have at least one copy of this study, available in both hard-copy (three volumes) and CD-ROM. To obtain a copy, communicate with Mr. Steve Foster, Deputy Director, MCIA, at (703) 784-6140.

#### **7008. Marine Corps Reserve**

The Marine Corps Reserve represents a very significant source of open source expertise. Many Marine Corps Reserve personnel have achieved considerable stature as civilian experts in various regional and subject matter areas. Many have worked overseas as civilians, and acquired foreign language and foreign culture expertise which may not be a matter of record but which qualify them as "virtual" Foreign Area Officers.

MAGTFs should consider initiatives to identify specific Marine Corps Reserve personnel competent in languages and countries of direct interest to the MAGTF, so as to hold these Reservists as "hip pocket" augmentation unit for specific contingencies. As a general rule, the reservists who are most talented and most competent will not be available for "make work" active duty assignments or Individual Mobilization Augmentee billets, but would be available for 15-30 assignments in their country of interest.

Such reservists can be requested and funded apart from the normal Marine Corps Reserve funding process, by requesting General Defense Intelligence Program (GDIP) Reserve Augmentation funding from HQMC. When requesting orders for such reservists, ensure that the request specifies that a) liberal civilian grooming and attire authorized; b) non-reporting orders; and c) special conveyance authorized. The first permits the Reservists to blend in as civilians as they "walk the ground" legally; the second avoids any unnecessary

contact with the U.S. Embassy and precludes the Reservists from being co-opted for administrative duties by the local defense attache; and the third permits them to take in-country tours with guides, as well as hire canoes, donkeys, and other conveyances requiring an indigenous driver.

#### **7009. Additional Open Source Training Opportunities**

There is only one significant private sector source of open source intelligence training expertise, and that is OPEN SOURCE SOLUTIONS, Inc., the non-profit educational corporation dedicated to studying and teaching open source intelligence. This organization offers three significant additional open source training opportunities:

a) Annual Conference. Each year in mid-September, OSS, Inc. offers a 3.5 day conference on open sources, systems, and services. This conference, the only one of its kind, attracts between 600-800 international representatives (although 50% of the audience is from the U.S. government), and includes the Open Source Coordinators for all of the major European nations as well as many Asian and African nations. For information about the conference send electronic mail to <OSS96@oss.net> (change year as appropriate); send a facsimile request to (703) 242-1711, or call (703) 242-1700 and leave a complete mailing address.

b) Newsletter. *OSS NOTICES* is the only newsletter in the world dedicated exclusively to open source intelligence, and it draws on a substantial range of other publications to report each month, in 30-40 pages without advertising, on open sources, systems, and methods. Each month's issue has a theme, including six regional themes a year. To review past issues, visit <<http://www.oss.net/oss>>, email <[oss@oss.net](mailto:oss@oss.net)> with a request for a sample copy, or fax (703) 242-1711 with a request and complete mailing address.

c) References. OSS, Inc., which is now entering its fifth year as the leading advocate and student of open source practices, publishes a two volume *Proceedings* from each of its annual conferences, and these are available for purchase. Especially recommended is the set from 1995, which consists of *Open Source Intelligence: Selected Readings* (Volume I) and *OSS '95: The Conference* (Volume II).

The Community Open Source Program Office has in August 1995 released a Request for Proposal for a series of training lessons oriented toward the Open Source Information System, and these will be available no earlier than 1998 and perhaps later.

Any questions? Mr. Robert D. Steele, President of OPEN SOURCE SOLUTIONS, Inc., and a former Marine, is prepared to support any MAGTF in any clime and place. Communicate with him at <[ceo@oss.net](mailto:ceo@oss.net)>, voice: (703) 242-1700, or fax: (703) 242-1711.

## APPENDICES

	Page
A	White Paper on "Open Source Intelligence: What Is It? Why Is It Important to the Military?" 099
B-1	Talking Points on "Private Enterprise Intelligence: Its Potential Contribution to National Security" 110
B-2	Complete Paper on "Private Enterprise Intelligence: Its Potential Contribution to National Security" 113
B-3	Glossary 145
B-5	Core Open Source References 146
C	White Paper on "ACCESS: Theory and Practice of Intelligence in the Age of Information" 147
D	Concise Directory of Selected International Open Sources & Services 165
E-1	Internet: Self-Guided Tour 174
E-2	Internet: Intelligence-Oriented List of Useful Internet Sites 181
E-3	Internet: Intelligence-Related Sites from <i>PC Magazine</i> 190
E-4	Internet: How to Find an Interesting Mailinglist 193
F-1	Expeditionary Environment Research & Analysis Framework & Model 201
F-2	Mission Area Factors Summary 252
G	OSINT OPSEC: Selected References and Information 302
H	Expeditionary Factors Study: List of Countries 306

## **APPENDIX A**

### **Open Source Intelligence: What Is It? Why Is It Important to the Military?**

**Robert D. Steele, President  
OPEN SOURCE SOLUTIONS, Inc.**

#### **Introduction**

This White Paper defines Open Source Intelligence (OSCINT) and its relevance in meeting the needs of the military (both commanders and defense policy-makers).

OSCINT is intelligence derived from public information--tailored intelligence which is based on information which can be obtained legally and ethically from public sources.

This White Paper suggests that OSCINT is a both force multiplier and a resource multiplier. OSCINT provides a practical political and military advantage which complements the advantage provided by traditional intelligence, it is available at low cost, and it cannot be ignored.

First the paper describes and discusses the utility of OSCINT in general terms, and at the strategic, operational, tactical and technical levels of warfare, including a single practical example at each level. The paper then describes the "information continuum" within which a range of open sources, systems, and services can be obtained which are relevant to military needs. Finally, the paper provides a brief discussion of the status of the open source intelligence programs in the United States, The Netherlands, and Sweden, and concludes with a concise discussion of opportunities and risks inherent in the use of OSCINT to meet military requirements, and of several practical steps that can be taken to exploit OSCINT in support of military strategy, operations, tactics, and technical acquisition and countermeasures.

The official definition of OSCINT by the U.S. Intelligence Community:

By Open Source we refer to publicly available information appearing in print or electronic form. Open Source information may be transmitted through radio, television, and newspapers, or it may be distributed by commercial databases, electronic mail networks, or portable electronic media such as CD-ROM's. It may be disseminated to a broad public, as are the mass media, or to a more select audience, such as gray literature, which includes conference proceedings, company shareholder reports, and local telephone directories. Whatever form it takes, Open Source involves no information that is: classified at its origin; is subject to proprietary constraints (other than copyright); is the product of sensitive contacts with U.S. or foreign persons; or is acquired

through clandestine or covert means<sup>1</sup>

The official definition is limited in its understanding to standard commercial sources of traditional information, and excludes, to take one important example, SPOT imagery. It also fails to take into account the importance of unpublished materials including electronic information and human knowledge which can be accessed legally and ethically.

The official approach to OSCINT is also limited in that the existing information-handling architectures for intelligence processing, including dissemination to the commander, are all classified, and there is a very limited capability for routing unclassified information efficiently, even assuming it can be obtained. In most communities, there appears to be a reluctance to assume primary responsibility for the collection and processing of OSCINT, which is why military operators in two countries (the United States and the United Kingdom) are examining means of acquiring and exploiting OSCINT directly, bypassing the intelligence community in order to give action officers at the policy level, and commanders at the operational level, direct access to OSCINT.

Experienced intelligence professionals have found that while OSCINT is not a substitute for traditional intelligence disciplines, including Human Intelligence, Imagery Intelligence, and Signals Intelligence. However, OSCINT does offer three major advantages for planning and conducting military operations:

-- When encountering requirements for military operations in the Third World or in support of humanitarian assistance and counter-terrorist operations for which intelligence collection priorities have not been high, OSCINT is frequently the only discipline able to respond rapidly (to include commercial imagery), and it provides the commander and his staff with a rapid orientation adequate for both developing initial planning packages; and for establishing collection requirements for the traditional intelligence disciplines.

-- OSCINT is also a means of achieving significant savings, in that many essential elements of information required by the commander and his staff can be acquired from commercial sources at a lower cost, in less time, than from classified capabilities, with the added advantages that OSCINT is often more up to date, and requires no political risk in its acquisition. *This permits classified intelligence capabilities to be focused quickly and effectively on mission-critical gaps, and avoids depleting or mis-directing these scarce resources—"do not send a spy where a schoolboy can go".*

-- Finally, OSCINT, whether it precedes or follows traditional intelligence collection, can protect national intelligence sources and methods by serving as the foundation for

---

<sup>1</sup> Although the original intelligence community report was classified SECRET, the definition and extensive commentary appeared in an unclassified document, *United States Marine Corps Comments on Joint Open Source Task Force Report and Recommendations (Working Group Draft Dated 6 January 1992)*, and portions, including the definition, were subsequently reprinted in *OSS NOTICES* Volume 2 Issue 9 (30 November 1994).

intelligence support to joint and coalition operations where it is not possible, or desirable, to reveal the capabilities and limitations of the traditional intelligence community.

### Open Source Intelligence and the Military

The availability and utility of OSCINT depends upon, and will vary, depending on the specific area of operations under consideration, and on two other factors: the level of warfare, and the point on the spectrum of conflict, from presence to general war, where the intelligence will be applied.

In general terms, OSCINT has significant potential as a source of intelligence support in terms of indications & warning, policy development, contingency planning, security assistance, weapon acquisition (design and countermeasures), joint and coalition operations, and tactical operations against new priorities such as proliferation. Finally, OSCINT is vital as a means of rapidly orienting the commander and serving as the foundation for collection management within the traditional intelligence disciplines.

At the strategic level:

-- OSCINT can provide indications & warning of both hostile intent, and opportunities for military advantage. Content analysis of multiple open sources such as regional newspapers from the Middle East, are often if not always more reliable foundations for estimating stability and instability, than reports from clandestine sources with a limited range of access and a personal perspective that biases their reporting.<sup>2</sup> OSCINT is especially valuable with respect to cultural and demographic intelligence, areas not generally well-covered by traditional civilian and military intelligence collection and analysis capabilities.

-- OSCINT can also provide very important geographic and civil generalizations which can significantly affect major military acquisition and design decisions. For instance, most countries build their aircraft for optimal performance on a "standard aviation day" which is defined in terms of warm (60°-70°F) conditions and balanced humidity. The military commander that is responsible for expeditionary operations to the Third World will find themselves utilizing aircraft which carry half as much half as far because the standard aviation day in the Third World is hot (over 80°F with high humidity). If aircraft cannot be designed for optimal performance on a hot day, then the military commander can at least ensure that doctrinal publications reflect accurate load and lift capabilities for the true expeditionary conditions to be encountered.

-- OSCINT can provide unclassified threat intelligence which can be used to educate

---

<sup>2</sup> This point was made publicly by Dr. Stephen Fairbanks, the Iranian Analyst for the U.S. Department of State's Intelligence and Research Bureau, in the presence of his superior, Dr. Jennifer Sims, Deputy Assistant Secretary of State for Intelligence Coordination.

and mobilize public and political support for military needs including policy development.

At the operational level:

-- OSCINT can provide the geographic and civil generalizations required for regional force planning and force employment. In particular, OSCINT has establish credible regional generalization regarding the capabilities of air, ground, and sea forces to be encountered by the commander; geographic generalizations with respect to cross-country mobility, average line of sight distances, temperatures, and water availability; and civil generalizations such as bridge-loading, port clearance, airhead bunkering; and civil communications and computing resources. OSCINT provides a time-sensitive solution to questions the theater commander will have about civil infrastructure, political cliques and personalities, and economic or financial factors affecting operational employment of forces, and is therefore especially helpful to contingency planning which must be pursued without adequate support from traditional intelligence capabilities.

-- OSCINT is especially useful to the theater commander for the coordination of joint and coalition operations where traditional classified intelligence capabilities are either not available (e.g. in much of the Third World where lower priorities have restricted coverage), or cannot be shared with foreign elements.

At the tactical level:

-- OSCINT has been shown to be highly pertinent and effective against new priorities, including counter-proliferation, counter-terrorism, and peacekeeping operations. This is true for both conventional military operations focused on overt interdiction, and clandestine or covert "direct action" by special operations forces.<sup>3</sup>

-- OSCINT is a critical resource for the military commander who requires maps and digital targeting information for Third World area for which current geographic information is not available from government sources, whether classified or unclassified. In combination, SPOT and other commercial imagery resources can provide the commander with up to date maps containing all airfields, roads, and bridges; and soon containing contour lines as well,

---

<sup>3</sup> At a Canadian intelligence conference 27-29 October 1994, both the Director of the Canadian Security and Intelligence Service, Mr. Ward Elcock; and Dr. Paula Scalingi of the Los Alamos National Laboratory in the United States, stated that OSCINT provides over 80% of the input to the final all-source product; in Dr. Scalingi's case, this was with specific reference to intelligence support for counter-proliferation. Dr. Gordon Oehler, Director of the U.S. Intelligence Community's Nonproliferation Center, has made similar comments on several public occasions.



for expeditionary operations.<sup>4</sup>

At the technical level:

-- OSCINT about civil communications and computing capabilities in the area of operations will be very important to the commander. As information warfare and information peacekeeping become critical mission areas, and all opponents achieve some capabilities to conduct electronic warfare, the commander will need to use OSCINT both to understand how to degrade the performance of civil capabilities being used by opponents, and to consider exploitation of civil capabilities to maintain joint and coalition communications.

-- OSCINT will provide most of what the commander needs to plan and coordinate joint and combined air, sea, and land operations in the expeditionary environment, with specific reference to strategic airlift and sealift operations involving civil aircraft, air traffic control and air defense planning for civil platforms, and fueling and other logistical considerations.

### The Information Continuum

There are three ways of understanding the robust nature of the private sector's potential contribution to military intelligence needs. The first is by examining in general terms this continuum.

Schools	Libraries	Private Investigators Information Brokers	Government	Intelligence
<hr/>				
Universities	Businesses	Media	Defense	

Each of these nine sectors of the global or national information community maintains a cadre of human experts as well as a range of both hard-copy and electronic information. Much of what is known to them, or stored by them, is not available through commercial online services. Following a specific example from each sector:

---

<sup>4</sup> SPOT is going to 5-meter resolution imagery in the very near future. In the U.S. Space Imaging, Inc., a subsidiary of Lockheed, has announced plans to provide 1:2,500 meter synoptic resolution imagery, within a year. These commercial capabilities will be critical to expeditionary operations in the Third World because of the lack of current maps. One U.S. study, *Overview of Planning and Programming Factors for Expeditionary Operations in the Third World* (Marine Corps Combat Development Command, March 1991), determined that for the 69 countries of concern to the Marine Corps, there were no 1:50,000 combat charts for 22 of the countries, old 1:50,000 charts for ports and capital cities only in the case of another 37 countries, and very old 1:50,000 complete coverage for another ten countries.

-- Language schools can rapidly identify individuals by location and nationality who have received training in the home country language and are target country nationals (e.g. Somalis studying French in Paris): these individuals can be contacted and offered part-time employment as translators.

-- Universities utilize their existing infrastructures and a regular supply of cheap intellectual labor to maintain important and authoritative databases. The Monterey Institute of International Studies, for instance, maintains the best database on the proliferation of nuclear materials, and utilizes graduate students fluent in Russian, Chinese, Arabic, and other languages to cover a wide range of multi-lingual publications, and to maintain an electronic database, at very low cost.

-- Libraries can be used, either as needed or in a deliberate fashion, to serve as repositories for "just in case" archiving of political-military, economic, and other materials pertaining to specific countries. This allows the government to share the cost of archiving with other library sponsors, and in many cases avoid the cost all-together.

-- Businesses have enormous repositories of market research, including communications and logistics research, on countries throughout the world where they have made or plan to make an investment. Businesses are also acutely familiar with the political corruption, climate conditions, and other factors which affect operational efficiency in specific locations. Two unique examples of business dedicated to meeting private intelligence needs are Oxford Analytica, with its network of 750 overt agents world-wide, and *The Economist* Intelligence Unit.

-- Information brokers can be identified who specialize in particular scientific & technical topics or regions of the world. This permits more efficient search & retrieval by exploiting capabilities whose "learning curve" has been funded by others. In addition, information brokers can be identified with specific language capabilities, and employed to do rapid exploitation of captured or acquired documents.

-- Journalists responsible for specific areas of the world, including journalists specializing in military, aerospace, and insurgency matters, rarely publish ten per cent of what they know, and they never publish their sources. They can, however, be engaged to prepare special reports, and to provide background information on specific personalities of importance to planned military operations. This need not be done secretly or through direct recruitment; it can be done discreetly as a private commercial transaction. Media organizations, such as Jane's Information Group, acknowledge that they publish less than 20% of what they know, in some cases to protect sources--they are however willing to do tailored confidential reports drawing on their complete range of sources.

-- Governments, including provincial and state governments, frequently have experts in agriculture or other trade-related fields who are familiar with specific areas of operation and the logistics as well as the key personalities. Embassies have personnel whose reporting

does not fully communicate what they know. Bringing key government personnel together for a week can quickly establish a foundation for collection management which the commander could not normally achieve through analysis of raw information.

-- Other intelligence organizations, including the "information and research" elements of the Vatican, the United Nations, and the International Red Cross, have global networks of reporting sources, including sources with special linguistic and regional skill, that can be drawn upon.

The third way of understanding the robust capability of the private sector is to consider the range of information services that are offered which are directly pertinent to military intelligence needs. These are listed in three columns:

Direct Observation	Document Acquisition	Telephone Surveys
Commercial Online Searching	Document Translation	Market Research
Current Awareness	Broadcast Translation	<i>Recruited Agents</i>
Experts On Demand	Multi-Expert Research	<i>Industrial Espionage</i>

Recruited agents and industrial espionage are not considered legal nor ethical within the private sector, but there are very competent organizations that openly offer such services, to include route reconnaissance and target identification services in third countries. In each of the above categories, it is highly likely that a private sector partner can collect, process, translate, and deliver open sources of intelligence able to make an important contribution to the commander's needs for information--and to do so in a cost-effective fashion which could not be duplicated by defense attaches or traditional military intelligence collection brigades.

The third way to understand the utility of the private sector for military intelligence needs is to take a case study, such as Somalia. In the absence of internally-available intelligence information, the fastest means of establishing an encyclopedic foundation for further collection management, and the fastest means of providing the commander with at least some useful information pending responses from the traditional intelligence disciplines, it by seeking out private sector experts and private sector databases. A leading scholar, a leading businessman recently returned from a tour as General Manager in Somalia, a leading journalist, and perhaps an information broker specializing in African information could be brought together and could quickly identify human, hard-copy, and electronic sources--including sources of digital geographic information--of immediate utility.

In one specific instance, supporting a wargame on Somalia, an individual playing the role of the United Nations commander was able to overcome the inadequacies of the U.S. intelligence community by making three telephone calls. Overnight, in Express Mail, at a *pro forma* cost of about \$5,000, the individual received:

- From Jane's Information Group, a spiral-bound volume containing a map of Somalia clearly marking the nine clan areas; a one-page order of battle for each clan (at a time when most intelligence analysts were thinking only of the old Somali army); and a one-paragraph precis with full citation for each article about Somalia published in any of the Jane's publications (including the excellent *Jane's Intelligence Review*) in the past two years. This constituted a superb orientation for both planning and collection management.

- From Oxford Analytica, twenty two-page reports suitable for Presidents and Prime Ministers, covering three topical areas: United Nations operations in Somalia, U.S. foreign policy toward Somalia; and U.S. operations related to Somalia. Again, a superb orientation on strategy and policy, in concise and immediately-usable form.

- From *The Economist* Intelligence Unit, a copy of the appropriate country risk report, which included important summary information on the logistics difficulties that would be encountered, including the limitations of both the port and the airfields for strategic entry.

#### Commentary on Representative National Approaches to OSCINT

Although OSCINT has always been part of the national and military intelligence process, in recent decades increased emphasis on technical systems and secret collection have tended to sharply reduce the amount of funding and the number of personnel dedicated to collecting and processing publicly available information. At the same time, the "information explosion" or "information revolution" has dramatically increased both the quality and quantity of the information available in the public sector. Today the commander can take a weather map of Bosnia off of the Internet, or exchange email with volunteer observation and listening posts in Bosnia.

Unfortunately, the reality today is that most intelligence communities are trained, equipped, and organized to collect and process secrets. OSCINT capabilities in both the civilian and military sectors of government have both atrophied where they existed, and also failed to keep up with the growth of private sector OSCINT capabilities.

- United States of America. The National Foreign Intelligence Board was recently briefed to the effect that while 99% of the \$28-35 billion dollars a year budget is spent on classified collection and processing, and only 1% is spent on OSCINT, OSCINT provides 40% of the all-source product. In one interview, the Deputy Director for Science & Technology of the Central Intelligence Agency stated that this latter figure was actually 70%. The major element of the U.S. intelligence community program is the Foreign Broadcast Information Service, which is under severe criticism for its continued emphasis on print

media exploitation, and its inability to master a wider range of open sources. In an attempt to gain control over the modest distributed resources being applied to OSCINT, the Director of Central Intelligence created the Community Open Source Program Office. This office is about to release a strategic plan for OSCINT, but it is limited to improving internal community access to open sources already collected. The Department of Defense program, for which the National Air Intelligence Center is the executive agent, builds on the existing scientific & technical intelligence document acquisition and translation program. The Department of Energy Laboratories, and especially Sandia and Los Alamos, constitute a major OSCINT resource which is being exploited by some military consumers of intelligence, such as the U.S. Southern Command, but which is not under the control of the intelligence community. Some very modest individual initiatives have taken place within the military services, the most advanced of which is the publication, in draft form by the Army, of an open source primer for military intelligence officers. At this time the U.S. military does not have timely broad access to a full range of open sources.<sup>5</sup>

-- The Netherlands. Various open sources, including the *Intelligence Newsletter* out of Paris, and *OSS NOTICES* in the United States, have reported that the foreign and military intelligence agencies have been integrated. Within the new national intelligence agency, a special Open Source Coordinator has been appointed, and a task force approach is being taken to intelligence collection and analysis. Every task force has an open source intelligence specialist, and all requirements for intelligence must first be examined and if possible satisfied through OSCINT before tasking of clandestine or technical capabilities is permitted. More recently, the intelligence elements of the individual military services were integrated into a joint military organization reporting to the Prime Minister.

-- Sweden. This country is most interesting because it has a unique consortium within which to formally orchestrate the activities of government intelligence, the business intelligence community, and the university research community. Swedish scientific & technical attaches have been noted to regularly exploit the Internet, and there is discussion within Lund University of the need for an Open Source Intelligence Center™ to meet the combined needs of the government, business, and university communities in Sweden.

#### Advantages and Disadvantages of Open Source Intelligence

-- Advantages include the fact that OSCINT has virtually unlimited potential on any topic; is of relatively low cost because expertise is maintained at someone else's expense; is generally up to date; and can be shared with anyone.

---

<sup>5</sup> The extraordinary relevance of Department of Energy OSCINT capabilities in support of military operations are described in *SHARING THE SECRETS: Open Source Intelligence and the War on Drugs* (OSS Inc. Limited Edition, 1994). The Army paper, prepared by the 434th Military Intelligence Detachment, Strategic, is titled *Open Source Intelligence Resources for the Military Intelligence Officer* (Fort Huachuca, November 1994).

-- Disadvantages include the possibility of revealing military plans and intentions (security can be provided by laundering the question through trusted intermediaries); the time and cost associated with searching for exactly the right information within the huge volumes of public information; and the temptation to accept an open source at face value when it could be disinformation or simply inaccurate.

### Obstacles to Military Exploitation of Open Sources

There are three obstacles to military exploitation of OSCINT:

-- Organizationally, the military relies on a classified intelligence community for its "intelligence", and does not have an alternate structure established to obtain OSCINT. Among the most important problems created by this reliance are those of funding: there are no well-established programs for contracting directly with the private sector for OSCINT.

-- Culturally, there is a strong attitude, primarily within the intelligence community but to an extent within the operational community, that information achieves a special value only if it is classified. This is in part a result of a cultural inclination to treat knowledge as power, and to withhold knowledge from others as a means of protecting one's power. This attitude is the equivalent of the cavalry ignoring the tank and the machine gun. The "openness" paradigm has thoroughly defeated the secrecy paradigm, and those organizations which focus on protecting secrets rather than exploiting publicly available information, will find themselves "starving" for knowledge.

-- Technically, because of the historical focus on training, equipping, and organizing forces for unilateral and conventional military operations, with the added assumption that all "intelligence" will come through classified and well-established channels, the existing command & control architecture, including communications, computing, and intelligence elements, is not designed to rapidly interface with joint and coalition forces, with special forces and direct action clandestine teams, and with the vast array of private sector and non-military government elements which can provide OSCINT to the commander.

### Opportunities for Advantage

The Director of Military Intelligence (DMI) for any nation has essentially three opportunities to improve national capabilities to collect, process, and disseminate OSCINT to commanders and military policy-makers:

-- Existing library resources are poorly-funded and organized for the purpose of "just in time" archiving of information. Library resources, both within the intelligence community

and outside the intelligence community, must be recognized as the "source of first resort"<sup>6</sup> Commanders and policy-makers must restore funding for library operations, including the cost of subscribing to external online services and out-sourced research, while at the same time redirect the libraries toward "just in time" decision-support to specific consumers, and away from "just in case" generic collection and processing.

-- Existing military intelligence analysts must be given the training, fiscal authority, and commander's guidance necessary to convert them from narrow specialists focusing on the analysis of classified information, to managers of networks of overt human experts and related electronic and hard-copy databases. At the same time, analysts must be re-oriented so that their primary focus is on day to day interaction with the commander and other consumers of military intelligence, and on day to day collection management founded upon open source exploitation, rather than the existing focus on producing classified reports in isolation from the consumer.

-- Existing commanders, in consultation with the DMI, must recognize that it is impossible for the DMI to satisfy their intelligence requirements related to a wide range of new priorities, with existing classified military intelligence capabilities. The entire structure of military intelligence must be recast to permit rapid maneuver throughout the private sector's knowledge terrain, and the rapid collection, processing, and dissemination of mission-critical OSCINT to the commander at every level of operations (strategic, operational, tactical, and technical) and in "every clime and place".

### Role of the Military Reserve

The military reserve constitute a national resource which has enormous potential. A simple example will serve to make the point. For every country of interest, a cadre of five military intelligence reservists could be formed, and given a responsibility to monitor pertinent foreign language periodicals and publications (which would be provided them on subscription), and to prepare weekly OSCINT summaries. These same individuals should be afforded direct access to the Internet and commercial online databases, and serve as direct reinforcements on demand to the active duty military intelligence analysts responsible for the same areas of interest. Funds should also be provided for the five person cadre to spend thirty days each in the country of interest, unencumbered by administrative duties. In this way, when a contingency requirement emerges, the responsible commander can activate the appropriate cadre (or cadres in the case of a theater commander).

---

<sup>6</sup> This important phrase was developed by Mr. Paul Wallner, the first (and last) Open Source Coordinator in the Office of the Director of Central Intelligence in the United States. Mr. Wallner, a member of the Senior Executive Service (flag rank) served for many years in the Defense Intelligence Agency and has been a strong advocate for improving OSCINT support to the commander. Today he serves as Deputy to the first Director of Community Open Source Program Office, Dr. Joseph Markowitz.

## APPENDIX B-1

### PRIVATE ENTERPRISE INTELLIGENCE: ITS POTENTIAL CONTRIBUTION TO NATIONAL SECURITY<sup>7</sup>

#### Talking Points

##### Concepts

Threat: No longer mono-lithic, mono-culture.

Four warrior classes--high-tech brute, low-tech brute, low-tech seer, high-tech seer. Community was built to deal with high-tech brute, is not ready for the other three.

Must distinguish between data (raw print, image, signal), information (collated data of generic interest, including 95% of the intelligence community's production), and intelligence, which is information tailored to support a specific decision by a specific person at a specific time.

##### Context

Joe Nye's jigsaw puzzle analogy--OSCINT provides context and orientation, and larger share of the puzzle than before.

Information continuum (K-12, universities, libraries, business, private investigators and information brokers, media, government, defense, intelligence) is robust and ready to provide low cost responsive intelligence on many topics today.

Virtual intelligence community in U.S. is a \$500 billion per year industry, and *someone else pays the overhead*.

OSCINT is a means of achieving savings which permit reinvestment in improved clandestine and technical collection. *Don't send a spy where a schoolboy can go!*

---

<sup>7</sup> These talking points were prepared by Mr. Robert D. Steele, President of OPEN SOURCE SOLUTIONS, Inc., for presentation to a Canadian intelligence conference, "Intelligence Analysis and Assessment: The Producer/Policy-Maker Relationship in a Changing World. 27-29 October 1994, Ottawa, Canada.



## Challenge

Integrated analysis--integrating geographic and civil factors and striving for strategic and operational generalizations and forecasting, not just tactical and technical specifics about military capabilities--requires an order of magnitude increase in the exploitation of open sources.

90% of what the policy maker reads and listens to is not only unclassified, it is unanalyzed. Open sources reaching the consumer reflect a wide variety of competing influences and perspectives--the community is not helping the policy maker make sense of the babble.

"Just in time" intelligence support means just in time collection as well as production. Linear paradigm (consumer to analyst to collector to source, and back up) is dead. New paradigm is the diamond paradigm, where all four talk to each other at one time or another.

Must resolve the dilemma of whether intelligence is about secrets, or about informing policy. 80% of what is needed to inform policy is unclassified, and unclassified intelligence is much more useful politically.

## Change

We used to promote analysts for mastering classified data in isolation from open sources, collectors, and consumers. This will no longer be the case.

The analyst of tomorrow will be a manager of a network of overt human sources who serve as distributed filters of unclassified information, and provide "on demand" guidance as to the most pertinent sources and data.

The analyst of tomorrow will be a partial extrovert skilled at "recruiting" the consumer and maintaining direct personal relations with the consumer.

The analyst of tomorrow will be both a resource manager and a collection manager, able to draw from open sources to the fullest extent possible, while tasking clandestine and technical sources as needed.

## Country

The intelligence community cannot reinvent itself in isolation. To harness the distributed intelligence of the Nation and optimize its exploitation of open sources, the intelligence community--the Nation--requires a national information strategy.

That strategy should enable connectivity across the information continuum; nurturing and exploitation of distributed centers of excellence focused on content; coordination of information technology research & development; and establishment of Nation-wide standards of communications & computing security.

In the information age, only smart nations will prosper and survive. The intelligence community is a vital but not a sole source of national intelligence. The smart nation must integrated classified government capabilities with unclassified private sector capabilities to create a new form of national intelligence.

## **APPENDIX B-2**

### **PRIVATE ENTERPRISE INTELLIGENCE: ITS POTENTIAL CONTRIBUTION TO NATIONAL SECURITY**

Losing Our Way	114
OSCINT and the Changing Threat	118
OSCINT and Changing Definitions of National Security	122
OSCINT and the Consumer	124
The Strategic Context of Private Enterprise Intelligence	126
Operational Concepts, Policies, and Practices	131
Private Enterprise Intelligence--Tactical Opportunities	134
Conclusion	143
 Appendix B-3: Glossary	 145
Appendix b-4: Core Open Source References	146
 Figure 1: The Four Warrior Classes and Implied Intelligence Challenges	 118
Figure 2: Competing Influences on the Policy-Maker	124
Figure 3: The "Information Continuum" or "Virtual Intelligence Community"	29
Figure 4: Basic "Intelligence" Capabilities in the Non-Profit Arena	135
Figure 5: Core Business/Economic Intelligence Capabilities	138
Figure 6: More Intrusive Private Intelligence Capabilities	141

## PRIVATE ENTERPRISE INTELLIGENCE: ITS POTENTIAL CONTRIBUTION TO NATIONAL SECURITY

Robert David Steele<sup>e</sup>

*95% de l'information dont une entreprise a besoin peut s'acquérir par des moyens honorables.*

*Henry Stiller, Director General  
Histen Riller, Societe Civile*

**ABSTRACT:** *In an era when both the nature of the threat and the definition of national security have undergone radical redefinition, it is essential that the intelligence and security services understand what their consumers have recognized for many years: private enterprise intelligence capabilities are robust, diverse, responsive, and relatively inexpensive. As we all strive to "reinvent" our intelligence and security services, the potential contribution of the private sector must be understood and integrated into our final design. At the strategic level, the private sector provides the context for classified and technical collection; at the operational level, the private sector is well ahead of the government in pursuing new concepts for intelligence dominance; and at the tactical level, the private sector now offers open sources and services which can meet roughly 80% of the needs of traditional and emerging intelligence consumers.*

### Losing Our Way

Too often we in the intelligence community forget our roots and abandon our private sector allies. Spies existed before Christ, but most of them were actually legal travelers and

---

<sup>e</sup> *Mr. Steele is President of OPEN SOURCE SOLUTIONS, Inc., a non-profit educational association established to assist governments and private sector organizations in understanding and capitalizing upon private enterprise intelligence capabilities, generally known as "open source intelligence" (OSCINT). In 1992 he was named one of the "Microtimes 100: industry leaders and unsung heroes who made a difference in the computer industry in 1992 and helped create the future". In 1993 he was featured by Alvin and Heidi Toffler as "The Rival Store" in their chapter on "The Future of the Spy", in War and Anti-War: Survival at the Dawn of the 21st Century. Mr. Steele is a veteran of the clandestine service of the United States of America, has helped manage overhead satellite programs, and was the founding Deputy Director of the Marine Corps Intelligence Center, where he developed many of his findings on the relative utility of OSCINT as a substitute or complement to the traditional intelligence collection disciplines.*

discreet merchants. Tea was stolen from China, and porcelain from England, by merchants.<sup>9</sup> More recently Japan, China, and Taipei have demonstrated profitable and cost-effective private intelligence capabilities. France and Israel excel at government support to the private sector, but I speculate that soon it will be the private sector that is conducting most of the espionage as well as the open source intelligence (OSCINT) collection in these two countries.<sup>10</sup>

The Anglo-Saxon intelligence communities lost their way in the late 1950's, largely because of over-reliance on the American intelligence budget as a safety net, with the unfortunate result that the American tendencies to ignore counter-intelligence and cultural intelligence, and to rely on technical panaceas and bean counting, infected the other services and skewed the manner in which our respective intelligence services trained, equipped, and organized for sustained warfare against "the threat".

Among the worst of the American influences on Anglo-Saxon intelligence were its obsessive focus on the Soviet Union as the only enemy worthy of total attention; and the

---

<sup>9</sup> The "privatization of intelligence" is a concept--indeed a sub-discipline--which owes a great deal to Dr. Stefan Dedijer of Lund University in Sweden. His contributions were honored with a book dedicated to him, by Jon Sigurdson and Yael Tagerud, *The Intelligent Corporation: The Privatization of Intelligence* (Taylor Graham, 1992). Most recently, aided by one of his more promising disciples, Ms. Katarina Svensson, Ph.L., he published *Technical Anaches and Sweden's Innovation Intelligence* (Lund University, April 1994). It is not my task here to provide citations to the literature critical of classical intelligence, but I do wish to acknowledge the lasting influence of Mr. Loch K. Johnson, whose article "Seven Sins of Strategic Intelligence", *World Affairs* Volume 146 Number 2 (Fall 1983), and subsequent book, *A Season of Inquiry: The Senate Intelligence Investigation* (The University Press of Kentucky, 1985), set the stage for the critical exploration of alternative sources & methods. In the final note I provide several references focused strictly on private enterprise sources and methods.

<sup>10</sup> I consider the Swedes to be the "stealth Japanese" of the Anglo-Saxon intelligence world, and also--with the Dutch--to have the most potential for creating the first Anglo-Saxon "intelligent Nation". Outside the Anglo-Saxon world I look to India, Viet-Nam, and Saudi Arabia to set new standards of excellence in government and private sector intelligence endeavors, and in fact speculate that they have already enjoyed significant successes. The dark side of private enterprise intelligence is represented by the criminal gangs--where the Colombians have been relatively unsophisticated, but omni-present in shadowing every U.S. frigate and aerial observation aircraft, I see the Russian, Vietnamese, Korean, and Japanese criminal organizations as cohesive, well-funded, and highly sophisticated. They represent a major threat which law enforcement will not be able to handle without a radical redefinition of both the responsibilities of national intelligence, and the support obligations of national defense.

American "solution" for poorly managed human intelligence (HUMINT) against the Soviets", an extremely expensive and deceptively ineffective technical collection empire which had the unanticipated impact of precluding American HUMINT from developing into a serious clandestine service. A side effect of the American resort to extremely expensive and highly classified<sup>12</sup> imagery intelligence (IMINT) and signals intelligence (SIGINT) overhead collection systems was the abandonment of the robust, diverse, responsive, and relatively inexpensive capabilities of the private sector.<sup>13</sup>

---

<sup>11</sup> In the aftermath of World War II, the Americans displayed their distressingly usual tendency to take the easy way, and attempted to penetrate the Soviet Union using emigres and others from organizations which had already been thoroughly penetrated by Soviet intelligence. When all of these "agents" were captured and executed, rather than doing some serious soul-searching and then creating a more serious illegals capability, the Americans turned to the U-2 and its follow-on satellites as an "acceptable" alternative to traditional spycraft. Now we find ourselves facing a wide range of threats which are not amenable to technical penetration, while we are simultaneously handicapped by the absence of a clandestine service worthy of the name.

<sup>12</sup> Americans (among others) have developed the art of secrecy as a means of concealing ineffectiveness, inefficiency, and irrelevance. Although the technical disciplines, both imagery and signals, have much to offer our communities, the reality is that we process less than 10% of what we collect, and we disseminate roughly 10% of what we process (*ergo* we disseminate 1% of what we collect), and it is highly questionable as to whether the technical disciplines provide the return on investment that they should in comparison with either clandestine intelligence or open source intelligence. My detailed comments on the costs of secrecy is contained in my invited *Testimony and Comments on Executive Order 12356, "National Security Information"*, to the Presidential Inter-Agency Task Force on National Security Information, Department of Justice, 9 June 1994. For a related comment, consider the statement of Rodley B. McDaniel, then Executive Secretary of the U.S. National Security Council and a former Senior Director (White House) of the Crisis Management Center. Speaking to a senior executive service class at Harvard University, he stated: "Everybody who's a real practitioner, and I'm sure you're not all naive in this regard, realizes that there are two uses to which classification is put: the legitimate desire to protect secrets, and protection of bureaucratic turf. As a practitioner of the real world, it's about 90 bureaucratic turf; 10 legitimate protection of secrets as far as I'm concerned." As reported in Thomas P. Croakley (ed.), *C'I: Issues of Command and Control* (National Defense University, 1991), page 68.

<sup>13</sup> It was an enormous shock to me, while serving as the senior civilian responsible for the establishment of a new \$20 million intelligence production center, the Marine Corps Intelligence Center, to discover that the \$2 million per year we earmarked for a Top Secret Sensitive Compartmented Information (TS/SCI) computer system with direct access to data from the Central Intelligence Agency (CIA), National Security Agency (NSA), and Defense Intelligence Agency (DIA) proved to be virtually worthless. The analysts kept coming in

It is instructive, in thinking back to the early days of the Office of Strategic Services (OSS), to consider how very important the academics from the private sector were to the development of our analysis methods, and how very important open sources were to our strategic intelligence efforts. The anecdote about the price of oranges in Paris as an indicator of the effectiveness of our bombing attacks on the railroad bridges leading to Paris is a classic. In a more humorous and yet deadly serious vein, consider the story told by Miles Copeland, about how the OSS handled the innumerable requests from the Department of State and the Pentagon which did not merit clandestine collection.

The OSS put two men in a room with *The New York Times*. Anything that could be answered from this open source was typed up, stamped secret, and disseminated as the result of a highly compartmented human intelligence operation--and one which was ostensibly very expensive, hence justifying requests for additional funds. The information itself was not fabricated, only the purported methods of acquiring it.<sup>14</sup>

---

saying "there's nothing there but Soviet missile silo data, the Third World 'data fill' has not been done". I subsequently discovered that I could meet 80% of the intelligence requirements of the Marine Corps through the use of open sources, at a cost of roughly \$20,000 a year expended in subscriptions to LEXIS/NEXIS, EasyNet, Jane's Information Group, and several other private enterprise information services. Our first major product, for which I served as Study Director, was an unclassified review of 69 countries of interest to the Marine Corps. Titled *Overview of Planning and Programming Factors for Expeditionary Operations in the Third World* (Marine Corps Combat Development Command, March 1990), this product was unique for relying strictly on unclassified sources, and was embraced by the operational community because it a) asked them to define beforehand what they considered to be the key factors as well as the distinctions between high, medium, and low degrees of difficulty for each factor; and b) it could be easily shared with pilots and platoon commanders as well as coalition partners and the press. It was this experience that led to the subsequent Congressional interest and my launching of a public campaign--while still a government employee and with the approval of my General Officer--to radically realign resources between open and traditional sources of intelligence.

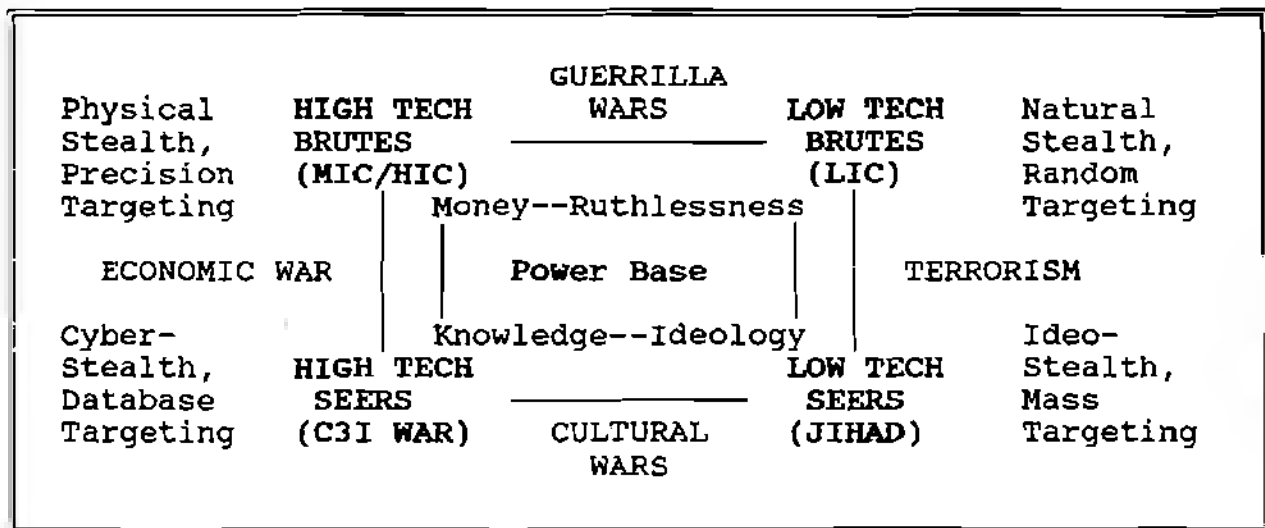
<sup>14</sup> Miles Copeland, *Without Cloak or Dagger: The Truth About the New Espionage* (Simon and Schuster, 1974), pp. 47-48. It was with great amusement that I listened to four recently retired KGB officers, speaking at OSS '93 on the topic of "Soviet Exploitation of U.S. Open Sources During the Cold War". To a packed room, they described how often "Centre" would catch them in the act of using open sources as a substitute for successful agent operations, and how open sources were in fact a mainstay of their Cold War scientific & technical collection efforts. Second International Symposium on "National Security & National Competitiveness: Open Source Solutions", Washington, D.C., 2-4 November 1993. The officers speaking were Colonel Vladimir B. Barkovsky, Ph.D. (former Deputy Director, KGB Science & technology Institute); Colonel Yuri I. Modin, Ph. D. (former Deputy Director, Research Institute on Intelligence Problems); Colonel Vsevelod I. Gapon (former

OSCINT has maintained a modest role within the larger intelligence communities, and a more central role within the smaller intelligence communities, but the reality is that the Anglo-Saxon intelligence communities of today exploit less than 10% of what is available from the private sector.

It is our task to explore the larger strategic context within which private enterprise intelligence can make a contribution to national security; to understand operational concepts from private enterprise intelligence which can and should be adopted by the traditional government intelligence services; and finally, to inventory, at this point in time, some of the specific private enterprise intelligence capabilities which can be used by the government to achieve both tactical results and sustained savings.

### OSCINT and the Changing Threat

Others participating in this conference have addressed the changing threat and changing intelligence agenda, but I wish to outline here an intellectual construct which influenced my early appreciation of how poorly our intelligence community exploits private sector intelligence capabilities, and how relevant OSCINT is to the threats that have always been with us, but which are receiving a more appropriate degree of interest today.



**Figure 1: The Four Warrior Classes and Implied Intelligence Challenges<sup>15</sup>**

Deputy Chief of Division, KGB): and Colonel Yuri H. Totrov (former KGB Section Chief for Counterintelligence, Central Intelligence Agency Affairs).

<sup>15</sup> This graphic is from my article "The Transformation of War and the Future of the Corps" in *INTELLIGENCE: Selected Readings--Book One* (Marine Corps Command & Staff College, AY 1992-1993). It is my privilege to continue serving the Marine Corps as Adjunct



While there are obviously variations to these four categories (for instance, some international criminals now use very sophisticated Swiss encryption and communications devices, as well as computer Van Eck emissions capture devices), these four categories helped me focus on the original threat--the high tech brute or conventional military opponent --while also keeping sight of the three major emerging threat categories.

What I perceive in this matrix is two fundamental aspects of national security and national intelligence:

a) First, since the National Security Act of 1947 which created the U.S. intelligence community, all that has followed has led to an intelligence community trained, equipped, and organized to deal with a single monolithic "high-tech brute", the Soviet Union, and very poorly trained, equipped, and organized to deal with smaller high-tech brutes, such as Iraq, or the other three major categories of threat. In particular, national intelligence capabilities in support of both international and domestic law enforcement, and economic competitiveness, are mediocre to non-existent.<sup>16</sup> We do not have the long-term ethnic human penetrations we need against international criminal organizations, nor do we have the kind of tactical SIGINT capabilities, or even air-breathing tactical IMINT, that would be helpful in coping with this robust international cancer.<sup>17</sup> We find that cultural movements baffler our

---

Faculty for Intelligence. My thinking was stimulated by Martin Van Crevald during his tenure as a Visiting Professor at Command & Staff College, and by his book *The Transformation of War* (Free Press, 1991).

<sup>16</sup> For a detailed critique of the existing U.S. intelligence community, a critique which draws on my years of service both in the Central Intelligence Agency as well as the Marine Corps, including participation in all of the post-mortems on intelligence failures in the Gulf War as well as Marine Corps support to the Department of Defense "reinvention of intelligence" initiatives undertaken by then Assistant Secretary of Defense for Command and Control, Communications, Computing, and Intelligence, Mr. Dwayne Andrews, see "A Critical Evaluation of U.S. National Intelligence Capabilities" in the *International Journal of Intelligence and Counterintelligence* (Volume 6, Number 2, Summer 1993). More recently I have summed up four years of critical commentary in "Reinventing Intelligence: Holy Grail or Mission Impossible?", in the *International Journal of Intelligence and Counterintelligence* (Volume 7, Number 2, Summer 1994).

<sup>17</sup> Until recently, very few traditional intelligence analysts were aware of the existence of the International Association of Law Enforcement Analysts (IALEA). This organization represents a first step in transferring some of the methods of analysis developed by the traditional intelligence community into the law enforcement arena. They can be reached at Post Office Box 52-2924, Miami, Florida, 33152, Voice: (305) 653-3010, Facsimile: (305) 716-3218. When I participated in reviews of intelligence effectiveness against low intensity conflict targets, one of the most critical deficiencies was the fact that our systems could not deal with "low slow singleton" targets. A major deficiency within the military is its

indications & warning (I&W) system because they do not use point to point communications but rely instead on couriers, the pulpit, and broadcast television to indirectly mobilize action elements from within the masses.<sup>18</sup> We do not have an electronic counter-intelligence capability worthy of the name, nor have we established the most basic economic counter-intelligence capabilities.<sup>19</sup>

b) Second, and this stems from a personal awaking inspired by the failure of our Marine Corps Intelligence Center's \$10 million classified intelligence computing system and related classified databases, when contrasted with a \$20,000 a year expenditure on private enterprise information sources and services, it is clear to me that OSCINT can meet 80% of our needs for intelligence against the emerging threats, and that OSCINT must be the foundation upon which we completely restructure our classified capabilities.

Now, there is going to be a natural tendency on the part of the "old boys" to say that OSCINT is all well and good, but not for critical national security issues. I have heard this from the best of them, including flag officers in England and France. I have also heard from flag officers in the U.S. and England, and officers in other countries, that they are fed up with classified intelligence that is relatively useless to their day to day needs, and highly interested in streamlining and improving their direct access to private enterprise information

---

propensity to procure "fast movers" (jets) with very limited loiter times over the target area. at the same time that they decline to invest in the necessary "sensor to shooter" collection and connectivity so that these expensive toys can be effective against low slow singletons targets.

<sup>18</sup> One of the finer pieces of journalism I have encountered was a superb series, each article taking up an unheard of full newsprint page or more, in *The Washington Post*. On Monday 2 August 1993 they published "Islamic Warriors: Radical Movements Thrive on Loose Structure, Strict Ideology", and a sidebar article, "Militarized Hezbollah Follows Lead on Iran". On Tuesday 3 August 1993 they published "Islamic Warriors: Global Network Provides Money, Haven", with a sidebar article on "A New Strain of Terrorism: Groups are Fast, Loose, Hard to Find".

<sup>19</sup> Many of my thoughts on information warfare, and information peacekeeping, are contained in my lecture "War and Peace in the Age of Information", presented by invitation to the Naval Postgraduate School at Monterey, California, as a Superintendent's Guest Lecture on 17 August 1994. Among other controversial elements, this lecture outlines how I would completely neutralize U.S. military and civil capabilities through electronic attacks on ten specific targets. More recently my friend Winn Schwartau has published a superb book, *INFORMATION WARFARE: Chaos on the Electronic Superhighway* (Thunder's Mouth Press, 1994), a detailed review of the specific capabilities and threats associated with personal, corporate, and global information warfare.

sources.<sup>20</sup>

Let me offer just two short proofs. In 1991 over 100 senior officers, including ten Colonels from the Marine Corps (an unheard of investment for a single event from this

---

<sup>20</sup> For a current critique of the U.S. intelligence community by a prominent consumer, see former Secretary of State George P. Shultz's *Turmoil and Triumph: My Years as Secretary of State* (Charles Scribner's Sons, 1993), pp. 50, 297, 307, 312, 425, 492, 493, 595, 619 *passim*. One Marine Corps general officer has stated that he used to talk about intelligence being broken, until he realized that this implied it existed--in his view, national intelligence simply does not "exist" when it comes to supporting expeditionary military operations. I am fully familiar with the open source intelligence capabilities of the U.S. intelligence community, and in fact served as the Marine Corps member of the Open Source Intelligence Council until my resignation from the Corps on 1 April 1993. The Foreign Broadcast Information Service (FBIS) and the excellent scientific & technical intelligence capabilities developed by the National Air Intelligence Center (NAIC), the National Maritime Intelligence Center (NMIC), and the National Ground Intelligence Center (NGIC) all merit respect. Unfortunately, the U.S. intelligence community spends less than 1% of its budget on open sources (while admitting that open sources provide 40% of the all-source product), and is in my judgement tapping less than 10% of the private sector's capabilities. Among the obstacles to improved OSCINT are an archaic security system, a culture that thrives on secrecy rather than results, and a procurement system that makes it very easy to spend millions on hardware, while making it virtually impossible to subscribe to LEXIS/NEXIS or pay a consultant a quick \$1,000. I am totally committed to protecting and improving the U.S. national intelligence community, and attempting to preserve its present level of funding. but in the absence of radical realignments among the disciplines and between collection versus distributed analysis, the community is in for some rough years. The first community attempt at defining its open source intelligence strategy was so disappointing, without reference to past studies or known experts, that I was obliged, as a Marine Corps civilian, to produce *United States Marine Corps Comments on Joint Open Source Task Force Report and Recommendations: Working Group Draft Dated 6 January 1992* (Headquarters, U.S. Marine Corps, 11 January 1994). The intelligence community finally appointed an Open Source Coordinator, Mr. Paul Wallner, to whom I am indebted for his integrity in supporting our private sector advocacy of open source intelligence developments; more recently Dr. Joseph Markowitz has been appointed Director of the Community Open Source Program Office (COSPO), with Mr. Wallner as the Deputy for this much-expanded effort. I have a very high regard for both of these gentlemen--but they are not being given the inter-agency authority and resource control they require to truly make OSCINT "the source of first resort", as Mr. Wallner has correctly defined it. I do not believe the U.S. intelligence community will truly restructure until it faces the real threat of a 50% (fifty percent) cut in its budget over five years, a threat which may well materialize in 1994 as an outcome of the newly established Warner Commission (formally known as the Commission on the Roles and Capabilities of the United States Intelligence Community).

austere Corps). met at the Naval War College in Newport for Technology Initiatives Game 1991. This game was a first effort to scrub Admiral Jerry Tuttle's COPERNICUS program. and included an Intelligence Cell. Here is a paraphrase of what the Navy Wing Commander (Captain, O-6) who led the lead flight into Baghdad said:

*If it is 85% accurate, on time, and I can share it, that is a lot more useful to me than a compendium of Top Secret/Codeword information that is too much, too late, and needs a safe and three security officers to move it around the battlefield.<sup>21</sup>*

We in the intelligence community must be mindful of the acceleration of the operational tempo, and the fact that our consumers are not stupid. They are growing impatient with the ability of the intelligence community to "keep up". In the Gulf War the classified imagery cycle took eight days from articulation of the requirement to deliver of the imagery. The operational planning cycle was three to five days. Classified imagery was not only poorly suited for wide area surveillance, but it was always too late to be really useful. By contrast, you now have real-time imagery delivery from SPOT, and commercial synoptic one-meter imagery is a year or two away from reality. CNN is blanketing the battlefield, and although it is often wrong, it influences policy and operations. Commercial online services and international executive investigative services are offering astute consumers a degree of tailored intelligence support which is not available from the intelligence community for anyone other than the President or Prime Minister.

More recently, we have the instructive example of OSCINT in the war on drugs. Without belaboring the point, as an entire book will be coming out shortly on this topic. Los Alamos National Laboratory has demonstrated that for \$100,000, using only OSCINT, it can do better at estimating global drug production and movement than an equivalent effort by the U.S. national intelligence community, at a cost of \$12-15 million dollars.<sup>22</sup>

### **OSCINT and Changing Definitions of National Security**

With the globalization of demographic and ideological movements, as well as the globalization of crime and the economy, the intelligence community is finding itself hard-

---

<sup>21</sup> Marine Corps Trip Report, Technology Initiatives Wargame 1991, Naval War College, 21-25 October 1991, disseminated by Assistant Chief of Staff, Command and Control, Communications and Computer, Intelligence and Interoperability, Ltr C412R dtd 3 January 1992.

<sup>22</sup> Dr. James Holden-Rhodes, *SHARING THE SECRETS: Open Source Intelligence and the War on Drugs* (forthcoming), extract from Chapter 5. This book has been selected for distribution at OSS '94, and 1,000 copies will be especially printed by OSS, Inc. one year in advance of the book's release to the public by the prospective publisher.

pressed to meet the needs of its consumers for intelligence about areas which have traditionally been excluded from its charter, such as strategic economic intelligence assessments which must of necessity draw on comparative domestic economic information; or support to law enforcement in its increasingly dangerous efforts to contain very powerful and very ruthless international criminal organizations with solid ethnic cohesion.<sup>23</sup>

It was instructive to me, in January 1994, to hear Ms. Ellen Seidman, Special Assistant to the President of the United States, discuss her responsibilities on the National Economic Council, and her perceptions of both intelligence and normal governmental information processes. In brief, she found the intelligence community irrelevant to her mandate because in the U.S. the intelligence community is not permitted to develop strategic assessments about domestic matters, even economic competitiveness matters. At the same time, Ms. Seidman expressed frustration with the normal governmental information processes, such as represented by the Federal Reserve Board and the Departments of Commerce, Treasury, and Labor, because the latter do not have any concept of how to collect, process, and disseminate intelligence. They don't "do" collection management, or critical analysis, or forecasting, or indications & warning, at the level of sophistication which our intelligence communities have developed over time.<sup>24</sup>

As we reinvent intelligence, there is clearly a need to reconsider not only our sources and methods, but the range of inquiry and the broadness of the consumer base. In my judgement the intelligence community must find a new balance between supporting more consumers with non-traditional requirements including domestic information requirements, while also relying on open sources and private enterprises to fulfill most of the encyclopedic intelligence requirements. The intelligence community, cannot, however, centralize its management of OSCINT, nor can it even presume to control what reaches the consumer. There is a strategic approach which must be taken to integrate government intelligence with private enterprise intelligence.

---

<sup>23</sup> Mr. John Petersen, President of the Arlington Institute (and former staff member of the National Security Council) defines national security in this way: "The Nation's security is no more than the total of the individuals' perceived sense of security (at home and abroad)." He uses a matrix from "Here to There" and "Peace to War" to show the broadening of national security concerns to include "Here" and "Peace" as major areas where both our defense community, and our intelligence community, are not prepared. Personal communications.

<sup>24</sup> Ms. Seidman was speaking to the Open Source Intelligence Lunch Club in Washington, D.C. on 11 January 1994. Her remarks were reported in *OSS NOTICES* Issue 94-001 dated 21 February 1994, page 10.

## OSCIINT and the Consumer

As we consider how best to integrate OSCINT capabilities from the private sector with both old and new classified intelligence capabilities, we must remain acutely conscious of the realities which characterize our consumer's acceptance and exploitation of information.

<u>Politicians</u>		
Executive Leadership		
Legislative Leadership		
Personal & Professional Staffs		
<u>Government Officials</u>		<u>Foreign Officials</u>
Department Heads	P	<u>and Organizations</u>
Assistant Secretaries	O	Diplomats
Program Managers	L	Counterparts
Message Traffic	I	Correspondence
	C	
<u>Private and</u>	Y	<u>Independent</u>
<u>Public Sector</u>		<u>Researchers</u>
Lobbyists	M	Think Tanks
Executives	A	Academics
Citizen Groups	K	Authors
Polisters	E	Foundations
Individuals	R	Laboratories
<u>Media</u>	<u>Personal</u>	<u>Intelligence</u>
CNN/C-SPAN	Family	<u>Community</u>
Newspapers	Intimates	CIA
Wire Services	Church	NSA/DIA
Radio/TV	Clubs	State
Pool Reporters	Alumni	Services

**Figure 2. Competing Influences on the Policy-Maker**

Consider the above figure, a graphic depiction of the range of "open sources" reaching the consumer each day, independent of the intelligence community:<sup>25</sup>

<sup>25</sup> This chart is reproduced from "A Critical Evaluation....", *supra* note 8, and in turn taken from the CIA "Intelligence Successes & Failures Course" which I understand has been discontinued. Dr. Jack Davis, Senior Intelligence Service, was for many years the keeper of the flame for "real world analysis", and the only senior officer willing to stand up to those who would politicize intelligence analysis and pretend that going through the motions constituted real intelligence. Others whose integrity and vision merit recognition including

a) Ninety percent of what the consumer reads and listens to is not only unclassified, but also unanalyzed and unrelated to the classified information sent to them.

b) There is no penalty to the consumer for ignoring classified information.

c) Classified information often comes with so much security baggage as to be an untenable contender for the policy-level consumer's attention (and the executive assistants do not have the codeword clearances, so even the consumer's filtering mechanism is of no help in flagging "useful" codeword material).

d) Unclassified material, even if inaccurate, if it fits the consumer's worldview or agenda, is immediately useful as something which can be disseminated to the press, the public, or Parliamentary personalities.

One of the most important changes the intelligence community can make, one which both addresses the potential as well as the hazards of unbridled open sources reaching the consumer directly, is to develop a much more extensive network of analyst-operators assigned to specific consumers and attending directly to their daily needs. Only through day to day interaction, and physical co-location, will such intelligence community representatives be able to a) monitor the OSCINT reaching the consumer, b) earn the consumer's trust and confidence; and c) properly channel requirements for timely action by the classified world, and d) "pull" exactly the right intelligence from the classified world in such a way as to be directly pertinent to the consumer's needs of the moment.<sup>26</sup>

---

the instructors for the Harvard "Intelligence Policy Seminar", notably Drs. Ernest May and Richard Neustadt, and in recent years, including the course I attended, Dr. Gregory Trevorton (now Vice Chairman, National Intelligence Council). Mr. Doug MacEachin, the current Deputy Director for Intelligence (DDI) is a superb officer laboring under enormous constraints to improve intelligence analysis--as he has commented to a meeting of the Security Affairs Support Association, in paraphrase, "it is hard to do serious analysis when you have a bunch of 19-year olds on two year rotations". The entire concept of what constitutes the "value-added" role of national intelligence needs redefinition.

<sup>26</sup> The best article I have seen on how best to do intelligence analysis within the kind of competitive environment provided by OSCINT from private enterprises is that of Mr. Andrew Shepard, a senior analyst now on detail to the Community Management Staff (CMS). His "Intelligence Analysis in the Year 2002: A Concept of Operations", was published in the *Proceedings* (Volume I) of the First International Symposium on "National Security & National Competitiveness: Open Source Solutions" (McLean, Virginia, 1-3 December 1992), and is beginning to have an impact outside the United States. The paper was first presented at the Symposium on Advanced Information Processing and Analysis (Reston, Virginia, 24-26 March 1992). Mr. Shepard capably articulates how on-site intelligence analysts can fulfill three major roles in direct support of the consumer: real time validation and review of

## The Strategic Context of Private Enterprise Intelligence

When we lost our way in the late 1950's, and fell in love with technology and the simplicity of a world with only one "main enemy", we built ourselves a cement bunker with no windows. In their time, satellites were like an oasis in the desert. However, in the past twenty years private enterprise information collection, processing, and dissemination alternatives have exploded--unfortunately, for those within the bunker, with its bad air and depleting supplies, it is difficult to notice such changes. It is a tribute to the organizers of this conference, and those behind them, that OSCINT is receiving a full and proper hearing in Canada.

The strategic context of private enterprise intelligence is a fundamental starting point for the reinvention of intelligence. There is no more promising aspect of our profession than that offered by the private sector. While we must assuredly pursue improvements in both clandestine and technical collection sources and methods, OSCINT--the private sector--must of necessity serve as both the "stopgap" measure by which we meet requirements for which our community is not trained, equipped, and organized; and also the benchmark against which we evaluate the value of clandestine and technical capabilities applied to new targets.

In the tactical section which concludes this paper I provide examples of specific private enterprise information-intelligence capabilities from each of the above. At this, the strategic level, I wish to make three points:

a) First, the consumer is now in charge, and acutely conscious of the advantages which OSCINT provides, not only in terms of responsive information at a very low cost, but in terms of political advantage....OSCINT can be shared with the press and Parliament, and therefore is much more politically potent than a secret report which cannot be shared.

b) Second, this is the age of distributed information. It is simply no longer possible to centralize control over collection, storage, processing, and dissemination. I have stated publicly my view that the "Central" Intelligence Agency is not long for this world--that is not to say that we do not require its capabilities, simply that the way in which it is now organized and managed is so ineffective and inconsistent with the realities of today, that it must inevitably join the mammoths in the tar pit.<sup>77</sup>

---

OSCINT reaching the consumer independent of the intelligence community: real-time retrieval from intelligence community databases of that information which can be tailored to support an imminent decision by the consumer; and collection management tailored to the needs of the consumer rather than the circumstances of the collectors.

<sup>77</sup> My most detailed statement on where I see the U.S. intelligence community developing, to include the dissolution of the Central Intelligence Agency (and the establishment of a separate Clandestine Services Agency) is contained in *OSS NOTICES*



c) Third, it is simply not advisable, for both political and financial reasons, to render classified intelligence support to private enterprise with any consistency, or with an assured return on investment. In coming to this conclusion I draw on my participation in a special workshop within the Harvard Executive Program on Intelligence Policy (1991).<sup>28</sup> There is no question but that classified economic espionage is required to "illuminate the playing field" for the governmental policy maker. However, given the fragmentation of ownership, management, and employment of most international firms, defining a strictly American or strictly Canadian firm meriting the expenditure of taxpayer funds for classified intelligence becomes problematical. What I found most interesting, though, in thinking about this issue with my classmates, was my personal conclusion that the single best thing the government can do for national competitiveness is to nurture the growth of what Lee Felsenstein calls the

---

Volume 2, Issue 6, 30 August 1994). Among the highlights: dissolution of the Central Intelligence Agency; establishment of a separate Clandestine Services Agency (CSA) under total non-official cover; conversion of the Directorate of Intelligence into the cadre for an inter-agency series of intelligence centers under the oversight of the National Intelligence Council; creation of Deputy Directors of Classified Intelligence for Research & Development, and for Communications & Computing; integration of the National Reconnaissance Office (NRO) with the Defense Mapping Agency (DMA) to create a Defense Mapping & Reconnaissance Agency which contracts out 75% of its collection and production; expansion of the National Security Agency (NSA) charter to include monitoring of unencrypted cyberspace data and the establishment of a clandestine capability for inserting alternative transmitters into sites using unbreakable encryption; and expansion of the Defense Intelligence Agency (DIA) to manage a totally integrated Intelligence Corps which provides the military intelligence personnel to all military elements from the forward-most tactical element through the Joint Intelligence Centers (JIC) and into the Pentagon. A superb book on emerging governance principles for distributed networks is that of Kevin Kelly (editor of *WIRED Magazine*), *OUT OF CONTROL: The Rise of Neo-Biological Civilization* (Addison-Wesley, 1994). One of the concepts which Kelly articulates is that of "hive mind". In my own work I am pursuing ideas once articulated by Teilhard de Chardin and Quincy Wright, among others, with respect to what constitutes an "intelligent nation". I envision a "virtual intelligence community" which is 100 times larger and more encompassing than the existing intelligence communities; while such a community must by definition be "out of control", it is in fact far more effective and responsive to the needs of our consumers than the existing government intelligence communities (and their non-intelligence uninformative counterpart agencies).

<sup>28</sup> This course, sponsored by the Central Intelligence Agency, brings together approximately thirty general officers and their senior civilian counterparts, each at a point where they are about to manage the entirety of their organization's intelligence resources. As the second civilian in the very small Marine Corps intelligence pond, I benefitted from this opportunity around eight years earlier than I might have in a larger organization.

"information commons" of open source multi-media data."<sup>29</sup>

Let me expand on this concept for a moment. Our own Deputy Assistant Secretary of Defense for Intelligence and Security, Mr. Keith Hall, has stated clearly that while intelligence must of necessity rely on OSCINT for context, that intelligence is intended to collect secrets not available "by other means", and that OSCINT falls firmly within the category of "other means".<sup>30</sup> What we have here is a dilemma. On the one hand, we want the intelligence community to focus on secrets. On the other hand we have to keep the policy-maker informed, and find that 80% of the time OSCINT is better at informing policy than are secrets. What I believe we need is a new strategic definition of what constitutes "national intelligence"--our definition must provide for a distinction between classified governmental intelligence and unclassified private enterprise intelligence, while also providing for the integration of both under the national intelligence umbrella.

The isolation of the intelligence community from its consumers, and the arrogance of the intelligence community in presuming that it knows best who its consumers should be, and that it knows best whether secrets are better than open sources in any given instance, must be brought to an end.

In essence, it is not enough for the government to simply understand and take advantage of private enterprise intelligence. It is essential that the government have a national information strategy, and that it nurture what I call distributed centers of excellence. It is not enough to expect that the private sector will undertake the necessary collection and processing that is required--government must actively encourage, without controlling, such endeavors, and constantly monitor the state of its national information continuum.<sup>31</sup>

---

<sup>29</sup> Lee works at the Interval Research Corporation in Palo Alto, California, and can be reached at (415) 354-0857, fax (415) 354-0872, email <lee@interval.com>. Interval is Paul Allen's attempt to create a modern Xerox Parc.

<sup>30</sup> Mr. Hall provided his first public address on the relationship between intelligence and open sources to the Open Source Intelligence Lunch Club in Washington, D.C., on 9 August 1994. Mr. Hall, whose rich experience at the tactical level in military intelligence and at the Office of Management and Budget as well as on the Senate Select Committee for Intelligence makes him one of the most qualified senior leaders in our community, was the originator of the term "ASK-INT", and has over the past decade challenged intelligence collectors to determine if the information they want to use expensive methods to collect might not in fact be available for the asking.

<sup>31</sup> In the United States, the National Information Infrastructure (NII) was until recently focused strictly on connectivity. It was with some gratification that I finally heard him speak of the need to harness the "distributed intelligence of the Nation", a phrase I used in my address to OSS '94. He used this phrase when announcing the GII in Brazil, and again at the Public Interest Summit in Washington, D.C. on 29 March 1994.

Below I illustrate what I call the "information continuum". It is very important to note that the intelligence community is but one ninth of that continuum, and that existing security and procurement practices assure the complete isolation of the intelligence community from the other eight sectors. If one regards the intelligence community as the pinnacle of the national information continuum, then the most interesting aspect of reinvention is that associated with new responsibilities for the community--instead of simply collecting information and processing it in a centralized way, the community must now begin the process of nurturing distributed networks which are unwitting or benignly witting, and most assuredly not "under control".

*What I call the "information continuum" is the knowledge terrain within which government intelligence and corporate intelligence must operate:*

K-12	Libraries	Private Investigators Information Brokers	Government	Intelligence
<hr/>				
	Universities	Businesses	Media	Defense

**Figure 3: The "Information Continuum" or "Virtual Intelligence Community"**

It consists of our elementary and secondary schools, our universities, our libraries, all businesses and their information repositories, private investigators and information brokers, the media including the trade journal and scientific & technical media, governments down to the state and local level, all defense and law enforcement organizations, and the official and usually secret intelligence communities. I call these the nine sectors of the information continuum.

*IF we can harness this distributed power, then we can create a "virtual intelligence community" far more capable than the isolated communities now in existence.*

The good news is that this continuum provides a low-cost, flexible, and responsive "virtual research department" of extraordinary power and value. The bad news is that very few people know how to navigate this terrain, or how to break down the iron curtains between sectors, the bamboo curtains between industries, the plastic curtains between individuals.

In order to bridge the gap between what we have in the "real" intelligence community today, and what we might have in the "virtual" intelligence community of tomorrow, a national information strategy is an essential pre-requisite. Whether through legislation or through administrative fiat, there must be a concerted effort on the part of the government to harness the "distributed intelligence of the Nation".

In addition to the connectivity that comes with the National Information Infrastructure (NII) and its international extension, the Global Information Infrastructure (GII), three other elements are required to fully harness private enterprise intelligence:

a) There must be, fully independent from the intelligence community<sup>32</sup>, a National Information Foundation (NIF), modeled after the National Science Foundation (NSF), which nurtures distributed centers of excellence without attempting to control them or their content.

b) Expenditures for information research and development (both tools and content) must be coordinated to avoid duplicative or counter-productive investments (e.g. every major bank commissioning a separate market survey on Indonesia, or development of a desktop analysts' workstation).

c) Communications & computing security must be assured through national standards, testing & certification laboratories, due diligence legislation, and national education.<sup>33</sup>

In brief then, while the private sector provides a very robust foundation for reinventing intelligence, and private enterprise intelligence can today be exploited well beyond what the intelligence community is doing, only a national program and a national strategy which explicitly recognizes the distributed nature of private enterprise intelligence, and seeks to harness it, will yield the optimal value for national security and national competitiveness.

---

<sup>32</sup> There is no avoiding the fact that most private enterprises, be they commercial or academic, will simply not trust the intelligence community to "manage" or "control" their databases or their activities. The best way to harness the distributed power of the private sector is to create a National Information Foundation (or Institute) which is non-regulatory and distributes funds (rather than centralizes information) to "centers of excellence" chosen because of their focus on specific regions or topics of interest to the government. This would be a non-intrusive means of orchestrating capabilities. OSS, Inc. is in the process of obtaining from every U.S. Senator and Representative their nominations for centers of excellence in their respective States and Districts, as a pre-ambule to publishing the first national inventory of centers of national intelligence excellence in the private sector.

<sup>33</sup> Although I have had very good relations with major hacker groups since 1992, when they recognized me for "hacking the intelligence bureaucracy", it was not until this past year that I realized that absolute private security was an essential pre-condition to complete openness. In order to engender the kind of open exchanges that are needed in a distributed intelligence system, it is essential that individuals feel that they a) know who is on the other end with some certainty; b) will receive the original document without modification; and c) can rely on a digital cash payment being transferred if that is part of the exchange. It was this realization that led me to oppose the Clipper Chip, and to testify to the NII Security Committee on 15 July 1994.

### Operational Concepts, Policies, and Practices

At the operational level, which deals with top-level guidance of over-all intelligence efforts, rather than the specific research tasks common to the tactical level, I want to highlight some core concepts where I believe that the private sector is ahead of the intelligence community.<sup>34</sup>

**Decision-Support** is the only acceptable mission for intelligence. One must carefully distinguish between *data*, which is the raw text, image, or signal; *information*, which is collated data of generic interest, such as newspapers or research reports; and *intelligence*, which is information that has been tailored to support a specific decision by a specific person about a specific topic at a specific time and place.<sup>35</sup>

**Collecting Secrets** is not difficult if you focus on collecting them before they become secrets. The weakest link, and the cheapest and easiest to exploit, is the grey literature and human infrastructure responsible for doing research just before someone decides to label something proprietary or classified.<sup>36</sup>

**Cast a Wide Net.** The French steel industry worked very hard at competitor intelligence against other steel industries, and completely overlooked the plastics industry.

---

<sup>34</sup> Both the operational concepts and the tactical specifics which follow were developed for my keynote presentation to the Association for Global Strategic Information (AGSI) in Heidelberg on 14 June 1994. That speech, oriented toward strategic planners and senior executives in international business, was printed as "ACCESS: Theory and Practice of Competitor Intelligence", *Journals of AGSI* (July 1994). Both sections have been revised, to include alteration of some of the tactical elements, in order to be more meaningful to a government intelligence community audience.

<sup>35</sup> When I first began developing new concepts for analysis in order to make the very austere Marine Corps Intelligence Center as effective as possible, I undertook a review of all CIA and DIA production available to the Marine Corps from the preceding year. I was intrigued to discover that almost nothing produced by either of these two organization actually supported any specific decision. It was all classified information of generic interest, and of a broadcast nature. I also found that almost all the production focused on a specific topic, weapons system, or country, rather than producing strategic generalizations helpful to long-term assessments and the formulations of strategic plans.

<sup>36</sup> For a detailed articulation of my theory and practice of OSCINT, see "ACCESS: Theory and Practice of Intelligence in the Age of Information". This was prepared for a foreign government which is among the most advanced in exploiting legal and open sources and methods in support of its national competitiveness. The paper was published in Volume I of the *Proceedings of the Second International Symposium on "National Security & National Competitiveness: Open Source Solutions"* (Washington, D.C., 2-4 November 1994).

which was busy developing steel substitutes.<sup>37</sup>

**Openness versus Secrecy.** The openness paradigm has won. The example of the nuclear industry, based on secrecy and not very progressive, is instructive when compared with the openness of the electronics industry, where competing engineers compare their approaches over coffee.<sup>38</sup>

**Just in Time versus Just in Case.** Paul Evan Peters, Executive Director of the Coalition for Networked Information, makes the point that in the age of distributed information easily accessible through electronic connectivity, it makes no sense to store volumes of out-of-date information when you can reach out and get exactly what you need in the way of current information on a "just in time" basis.

**Leverage Everyone Else's Overhead.** An expansion of the above concept is that of avoiding the enormous costs of attempting to maintain, with limited sustainability, in-house experts and in-house archives on everything. The private sector contains many superb information and intelligence capabilities where the resident expertise, and the existing databases, are maintained at someone else's expense. The intelligence community must do a much better job of exploiting such centers of excellence. *The most important contribution these external elements can make is not as a substitute for in-house analysis and the final production of an integrated classified product, but rather as self-sustaining information filters and on-demand experts able to rapidly identify the latest and best multi-media information pertinent to a specific decision area--information that can then be rapidly acquired, evaluated, and integrated.*<sup>39</sup>

---

<sup>37</sup> I heard this marvelous anecdote from Mr. Herve Serieyx, Vice President of the Institute for European Leadership, as included in his address to the French information industry congress, IDT '93, in Paris during the month of June 1993.

<sup>38</sup> Mr. John Perry Barlow, Co-Founder of the Electronic Frontier Foundation, articulated this contrast during his address to OSS '92.

<sup>39</sup> Early on in my OSCINT advocacy days, I suddenly realized that too many of my former colleagues were confusing my advocacy of OSCINT as a foundation for all-source intelligence with a view--which I do not support--that OSCINT can do it all or can substitute for clandestine and technical collection. I am fond of the analogy that Dr. Joseph Nye uses (he was until recently the Chairman of the U.S. National Intelligence Council). Dr. Nye talks about the intelligence problem as a jig-saw puzzle, and of open sources as the outer pieces of the puzzle, without which one can neither begin nor complete the puzzle. Clandestine and technical collection comprise the inner pieces. Dr. Nye would probably agree with my proposition that open sources have become a larger part of the solution in recent years--he might be reluctant to agree with my proposition that one often does not need the classified pieces in order to make a decision, and that in fact the maintenance of operational momentum is often in direct contradiction to the intelligence community's

**Diamond versus Linear Paradigm.** The old paradigm for information acquisition is the linear model, where the consumer goes to the analyst who goes to the collector who goes to the source, and then back up the chain the answer goes. This paradigm is not only too slow, it is not workable when you have a fast-moving topic with lots of nuances that are difficult to communicate to intermediaries. The new paradigm is the diamond paradigm, where the consumer talks to the analyst, the collector, and on many occasions the source, in order to ensure there is a timely and accurate meeting of the right minds<sup>40</sup>

**CIO = Corporate Intelligence Officer.** The last person corporations should appoint to the CIO position is the oldest information systems expert. They are technicians and do not have the slightest understanding of corporate strategy and the needs of senior executives for real-time *content* displayed in meaningful ways. The CIO position should not only be responsible for ensuring that the entire corporation—every employee—serves as part of the collection network, but also for ensuring that the information in hand is exploited, and that the corporation has the broadest possible network of external collection and processing capabilities on demand. The CIO should be the intelligence community's primary point of contact for legitimately and openly exchanging unclassified information.

**Information Value: content + context + time.** Corporations and banks have a wealth of information that is rotting away unused rather than being bartered or made available to one another as a means of increasing the competitiveness of an industry or a country. If

---

propensity to delay and delay in the hopes of getting a perfect answer. In forming my judgement on what best meets the need of my military commanders, I am influenced not only by many discussions with officers at the Warfighting Center of the Marine Corps, but also by Brigadier Richard E. Simpkin's excellent book, *Race to the Swift: Thoughts on Twenty-First Century Warfare* (Brassey's, 1985).

<sup>40</sup> I developed this concept while considering how relationships have changed between consumers, analysts, case officers, and clandestine agents. Those that do not actually understand the capabilities and limitations of clandestine intelligence frequently fall victim to the myths of clandestinity, and fail to understand that both agents and case officers are human. Too often, an agent will fabricate information or take information from open sources and pretend it comes from a "third cousin working for the Foreign Minister" to avoid any appearance of diminished access, and too often, a case officer will accept a fabricated answer either for lack of time to validate the information, or out of naivete. The number of case officers that do not read the local press or understand the local language at a level of competence sufficient to detect nuances and dissembling is distressing. Now, with so many open sources and so many experts being brought "on line" through the Internet and other means, it is my view that the role of the analyst is changing dramatically. Instead of evaluating analysts on the basis of their ability to master a limited amount of classified data, we must now begin training our intelligence analysts, and evaluating them, on the basis of their ability to identify and exploit an almost infinite range of external human sources.

one understands that stripping information of time and context allows it to be bartered without losing a competitive advantage, while gaining additional information in the process. then the way is open to operational-level agreements which will increase an individual firms competitiveness as part of a larger consortium. The intelligence community should be the catalyst for a national program to inventory existing information that is in storage or available through private enterprise collection networks, and then devising means of accelerating the transfer of basic information to the information commons.<sup>41</sup>

**Information-Driven Actions** are better than mission-driven actions. Many corporations as well as government organizations appear to be mired in old organizational practices where a business unit is given a specific series of tasks to accomplish, and is then expected to accomplish those tasks over and over again without reference to the external environment or other elements of the corporation.

**Corporate Hive.** Every employee is a collector, producer, and consumer of intelligence. Drivers of delivery vehicles, service technicians, those responsible for cold calls on customers, all should receive special training in observation and elicitation, and should have easy to use channels and processes for reporting what they see and hear. At the national level, the concept of "national hive" merits pursuit.<sup>42</sup>

In brief, then, we must think of each organization within the information continuum as an information network, with each citizen-employee being in turn responsible for exploiting those external information networks that they come in contact with--quite literally, everyone becomes a collection and producer of intelligence.

### Private Enterprise Intelligence--Tactical Opportunities

Now here are some tactical specifics--these are representative examples of capabilities that you could be using today--if you are not, you simply are not getting the best private intelligence possible.

---

<sup>41</sup> This concept of value probably owes something to a number of readings in cybernetics, but no single reading stands out. It was articulated in my paper on "ACCESS:....", *supra* note 25.

<sup>42</sup> See Kevin Kelly, *supra* note 16, *passim*. Kelly's book will be hard going for the average intelligence officer, but at the management level it is well worth the effort. The concept of gaining control over a \$500 billion a year private enterprise intelligence continuum by giving up control of the fraction of intelligence resources necessary to nurture distributed centers of excellence is one that will be difficult to accept for the current generation of senior intelligence managers, but one that will inevitably be implemented within the next five to six years by the incoming leadership.



I want to stress that reliance on a single provider of private enterprise intelligence and information services is no better than having an in-house capability--the greatest returns on your investments in tactical intelligence will come when you have the ability to "mix and match" sources and services from across the entire information continuum, hiring the very best experts on very narrow topics for only as long as needed, but with the assurance that the information they provide is first-hand, in-depth, and not only current, but in fact ahead of the published record.

It is also important to note that the non-profit arena, and particularly libraries, are discovering that they can exploit existing infrastructure, and cheap student labor, to compete with commercial online services. Across the information continuum, capabilities and limitations are in flux, with new and lower cost capabilities emerging every day.

<b>INTERNET</b>	Tony Rutkowski Internet Society (703) 648-9888	Brewster Kahle WAIS, Inc. (415) 327-9247	Chris Berendes Internet Navigator (202) 543-1527
<b>UNIVERSITIES</b>	Geoffrey Fox Syracuse "InfoMall" (315) 443-1722	U. of Michigan Clearinghouse <lou@umich.edu>	Economic BBS Rice University (313) 764-9366
<b>LIBRARIES</b>	Brenda Bailey Uncover Reveal (303) 758-3030	David Bender Special Libraries A. (202) 234-4700	Charles E. Bailey Jr Lib.-Oriented Lists (713) 743-9804

**Figure 4: Basic "Intelligence" Capabilities in the Non-Profit Arena**

**Tony Rutkowski**, Executive Director of the Internet Society, also oversees publication of a professional journal loaded with information about resources on the Internet, and understands better than most the technical issues associated with making global information available to any business. I am a member of the Board of Advisors of the Internet Society, and one of the things I am encouraging is a new focus on distributed content--on establishing a structured understanding of what comprises the "virtual library" or "virtual university" which is connected by Internet links.

**Brewster Kahle**, formerly with Thinking Machines, is the genius that invented the Wide Area Information Server (WAIS), which is now a standard for rapidly searching the entire Internet for weighted (relevancy ranked) full text documents. Brewster can tell you what businesses are doing to take advantage of the Internet, including their collection and search strategies. WAIS, and now the World Wide Web, enable an intelligence organization to constantly assess what is available on the Internet for any given topic, and to rapidly access

specific documents *and specific subject-matter experts.*"

**Chris Berendes** is a Master Inter-naut whose specific expertise is seeking out scientific & technical information of business value from all over the Internet.

One comment on the Internet: it eats people. It is much better to have a single Internet specialist, or to contract out searches, otherwise employees run the risk of either becoming hopelessly lost, or hopelessly addicted to wandering in cyberspace.

**Geoffrey Fox** is the man behind Syracuse University's "InfoMall". This is a good example of a university recognizing that it can substitute support to business for declining students as a source of revenue. He provides multi-media "intelligence" to businesses.<sup>4</sup> It is

---

<sup>4</sup> The economics of information, and the protocols associated with "tapping into" distributed expertise, are in great flux. Among those who are well-established within the Internet community, there is an understood barter economy as well as understood rules of behavior which preclude blatant exploitation (or even imposition of traffic upon) acknowledged experts. One of the most inconvenient things to happen to me is to have been listed in a new book, *E-Mail Addresses of the Rich and Famous*. While I am neither rich nor famous, my status as a former spy led to my being exploited by the publishers of this book, with the result that I must now deal with inquiries from people who have nothing better to do than send electronic mail to people they do not know. My rule of thumb is that I will give serious inquiries one free response--after that I charge \$200 an hour. Once small digital cash exchanges become a matter of routine on the Internet, I anticipate much more *ad hoc* consulting and self-publishing. One of the reasons that TELTECH and BEST America are doing so well is that they provide three essential services: they pre-screen experts for quality; they obtain non-disclosure agreements; and they handle billing and compensation. The private sector can be expected to develop many more clearinghouses and "expert on demand" capabilities meeting the needs of the intelligence community.

<sup>4</sup> Although intelligence communities have in the past exploited their universities, largely through directed contracts funded, in the United States, by "External Research & Analysis" (ER&A) funds, with the fiscal decline these funds have been among the first to be cut, a strategic error on the part of intelligence community management. It is far more productive to cut vertical slices of classified programs than to further distance the intelligence community from private enterprise intelligence capabilities. At the Advanced Information Processing and Analysis Steering Group (Intelligence Research and Development Council) Symposium in March 1993, one senior intelligence community officer lamented the fact that 80% of the information technology dollars go to maintenance, and that the installed base is dragging the whole program down. That is precisely the problem--the community needs to transition from an era of large centralized installed bases, and into an era where a core of dedicated analysts with the finest possible tools exploit private enterprise intelligence capabilities to the fullest extent possible--and only if the private sector cannot to meet the consumer's needs, should a

also a good example of how shared computing resources, and part-time university talent, can meet needs which the business and government communities might not be able to afford on a "full-time" or dedicated basis.

**University of Michigan Clearinghouse** for subject-oriented Internet resources is a classic example of graduate students doing something useful for the business community. Among the directories they have prepared are ones for aerospace engineering, government sources of business and economic information, and so on.

**Economic Bulletin Board Service** operated by the University of Michigan provides a number of useful files including statistical information, press releases from the U.S. Trade Representative, defense conversion information, East European trades leads, and so on.

I am convinced that universities, especially now that they are confronted with declining student populations, have a very important role to play in the provision of practical tactical intelligence support to corporations and governments. Adopt a university in order to harness the brainpower of their graduate students, and the connectivity and power of their electronic resources.

**Brenda Bailey** at Uncover Reveal is the tip of the Colorado library association that may put some of the commercial online services out of business. They are using existing library overhead to index and abstract, and then supporting their library services through on-demand faxing of materials for which fees are charged. Here is a simple example of their service: they distribute, at no cost via the Internet, the tables of contents of the journals they process. Any intelligence community analyst can receive, for free, exactly those tables of contents that are of interest to them--and they can either order copies of articles of interest from their government library, or--perhaps more efficiently, at a nominal cost from the University of Colorado.

**Special Libraries Association** takes care of the many corporate and academic special libraries, and in essence nurtures a wealth of information that is not mainstream but is very much at the heart of our national competitiveness. They are the private intelligence service for esoteric issues. They have been in existence for over 84 years, and specialize in helping librarians tap into international corporate libraries and other specialty collections.<sup>45</sup> The

---

revitalized clandestine or technical intelligence capability be called upon.

<sup>45</sup> One of the things that most impressed me during my March 1994 visit to Singapore, where I was welcomed by the National Computer Board (27 years olds with 140+ Intelligence Quotients, acting as a very effective shadow government), was their strategic plan to link government databases in the near future, *followed shortly by the linking of banks and private enterprise databases*. Obviously proprietary information and multi-level security issues will have to be sorted out, but I fully expect Singapore to be among the first three

Canadian equivalent of this organization should be an integral part of the national strategy for harnessing the enormous power resident in corporate libraries and databases.

Corporate and other private libraries are a critical national resource, and there should be a national program which facilitates "inter-library loan" sharing, as well as digitization of materials of common interest. My friend Paul Strassmann developed the concept of Corporate Information Management (CIM).<sup>46</sup> CIM means "one time data entry, corporate wide access". I have extended this concept to include National Information Management (NIM) and Global Information Management (GIM), and am convinced that the next major advance in the intelligence field will be the development of robust unclassified burden-sharing arrangements between governments and their private sector partners, and between governments acting on behalf of their private sectors....and of course in the private sector there are already numerous strategic alliances for information sharing.

**Library-Oriented Lists** on the Internet were put together by Charles E. Bailey, Jr. He is Assistant Director for Systems, University Libraries, University of Houston. He is Co-Editor of *Advances in Library Automation and Networking*, and Editor-in-Chief of *The Public Access Computer Systems review*. He understands the role libraries have to play in national competitiveness, and the importance of networking.

<b>BASIC PRIVATE INTELLIGENCE</b>	David Young Oxford Analytica + (44 865) 244-442	WONG Chiu-Yin <i>Economist Intel Unit</i> (212) 554-0600	Joseph Casitore FIND/SVP (212) 645-4500
<b>ADVANCED PRIVATE INTELLIGENCE</b>	Ruth Stanat SIS International (914) 639-1934	Herb Meyer RW1, Inc. (206) 378-3910	Dick Klavens SCIP (215) 896-4859
<b>PRIVATE INTEL CONSUMERS AND EXPERTS</b>	Olga Staios LEXIS/NEXIS (513) 865-7312	TELTECH Experts on Demand (612) 829-9000	BEST America Experts on Demand (410) 563-2378

---

"smart nation-states" in the world.

<sup>46</sup> Mr. Paul Strassmann is perhaps best known for his recent service as Director of Defense Information in the U.S., where he managed the world's largest information empire. Previously he has served in a number of executive positions, including Chief Information Officer of the Xerox Corporation. Among his recent books pertinent to the creation of national information architectures are *Information PayOff: The Transformation of Work in the Electronic Age* (Free Press, 1985), *The Business Value of Computers* (The Information Economics Press, 1990), and *The Politics of Information Management: Policy Guidelines* (forthcoming).

### Figure 5: Core Business/Economic Intelligence Capabilities

**David Young** founded Oxford Analytica, and this is, in my judgement, the finest global intelligence service that is open and private. He was a National Security Council staffer with Kissinger, and decided he could do better than what CIA was providing to the President. He enlisted the Don's of Oxford, and now provides the business community with daily intelligence and special reports that have earned praise from the World Bank and others. *Oxford Analytica runs 750 legal, overt human assets world-wide, trimmed down from an original 2,500 contract assets.*<sup>47</sup>

**WONG Chiu-Yin** runs *The Economist* Intelligence Unit, based in New York. They provide intelligence reports and special consultations to businesses world-wide, and there is a good reason why they are called an Intelligence Unit.

**Joe Casitore** is the Vice President for New Business Development at FIND/SVP in New York. This international firm will obtain any published document, including what we call gray literature (documents published in limited numbers by private parties, but not classified or proprietary). FIND/SVP also runs an "ask any question" service that is mainstay of the private intelligence business, and it has a strategic research division.

**Ruth Stanat** represents the best of the new private intelligence breed. She has an international company with correspondents all over, and she does a very fine job of both market research, and forecasting. Together with Herb Meyer and Kirk Tyson in Chicago, Ruth is among the best in the privatization of intelligence. David Young is my hero because he has a network of 750 agents worldwide, and does intelligence every day about every topic; Ruth does research on demand, but I believe she is a great deal more competent and more trustworthy than most private detectives and more globally tuned in than many information brokers. Ruth is also the author of the excellent book *The Intelligent Corporation: Creating*

---

<sup>47</sup> Every morning, the staff of Oxford Analytica meets, bringing together its area officers (one for each major region) with a changing mix of Dons. The area officers come to the morning meeting after a lengthy review of all over-night wires and news services. In collaboration with the Dons, they ask and answer three questions: a) where is the news wrong, and must be corrected for our clients? b) where is the news right, and must be elaborated upon with technical or other detail for our clients? and c) what weak signals are we starting to detect, that might allow us to make a useful forecast of coming changes for our clients? After deciding what issues to address that day, a limited number of their world-wide human network are mobilized. A typical example: a Chilean economist, friends with the Minister of Trade, is asked for a report. Within four hours he provides a two page report suitable for a President or Prime Minister, based on direct sourcing to those in positions of power. The World Bank complimented Oxford Analytica in writing, for being the only private enterprise to correctly forecast economic developments in Russia when it was transitioning from Gorbachev to Yeltsin.

*a Shared Network for Information and Profit.*

**Herb Meyer** is a good example of a "private spy" (in the new sense of legal open intelligence, not the old sense of industrial espionage). He was editor of *Fortune*, then Vice Chairman of the National Intelligence Council, and is now CEO of Real World Intelligence, Inc. He is the author of *Real World Intelligence: Organized Information for Executives*. Herb is a success story, and has translated lessons learned in the classified intelligence community into a competitive advantage in the private sector.

**Dick Klavens** is the President of the Society of Competitor Intelligence Professionals (SCIP). These are the people around the world whose specific job it is to collect, process, and disseminate corporate intelligence. They are the "in-house" managers of corporate-wide collection plans, cross-business unit intelligence sharing, and--when needed--the hiring of external information brokers, telephone surveyors, and the occasional (rare) private investigator. Their annual symposium, together with that of the Association for Global Strategic Information (AGSI), and that of the Association of Information and Dissemination Centers (ASIDIC), as well as my own, are "must attend" events for anyone who wishes to be follow the latest open sources & methods in the information age."

**LEXIS/NEXIS**, besides being a good all-around tool for research, is a good way of identifying experts and finding those journalists and professionals who are thinking about publishing the latest developments in specialized areas of interest.

**TELTECH** Experts on Demand are part of the private intelligence community, but they can also tell you about their customers. They have 3,000 technical experts on call, and can put a customer in touch with one over the telephone, with the result that "real-time intelligence" is produced when needed.

**BEST America** is similar to TELTECH, only they have 40,000 experts on line, and specialize in the life sciences. Pharmaceutical companies pay serious money to be able to reach out and tap into very narrow expertise on a moment's notice and with the assurance of total discretion.

---

<sup>48</sup> SCIP's symposium, including a number of excellent pre-conference tutorials, is generally held each April, and moves from city to city and attracts 500-700 participants. SCIP is actively expanding its international membership. AGSI meets in Europe and attracts 50-100 corporate strategic planners and business intelligence specialists. ASIDIC meets twice annually in the U.S. and attracts 50-100 of the leaders of the U.S. information industry. I consider ASIDIC to be the elite information industry association. The OSS symposium, the only symposium in the world where spys, hackers, information brokers, and corporate buyers of information services come together, is held in early November each year, always in Washington, D.C., and attracted 629 people in 1992 and 808 in 1993.

I want to emphasize the value of external experts. This is important because anything that is printed is by definition out of date. Books are seven to ten years out of date, articles are 7-10 months out of date, and even daily newspapers stories are a few days old. In the age of information, when speed is a factor in competitiveness, you can get ahead of the mainstream by using experts to create information and give it to you before it is published. Any research which does not commission original thinking and include some telephone surveys with real people is not optimized for advantage. Getting to the best expert on a topic, rather than relying on a generalist searching the literature, is the only way to ensure your research is current.

The external experts are especially important as uncompensated filters and evaluators. They spend their lives, at someone else's expense, monitoring their respective areas of expertise. In addition to providing their own expertise, they can quickly guide an intelligence community analyst to exactly the right materials, which can then be acquired for independent evaluation and integration into an all-source product.

<b>PRIVATE INVESTIGATORS</b>	Kroll Associates (New York) (212) 319-0044	Fairfax Group (Washington, D.C.) (703) 207-0600	Parvus-Jerico (USA-Bermuda) (301) 589-4949
<b>INFORMATION BROKERS</b>	Reva Basch Aubergine Info. Svc (510) 527-5770	Seena Sharp Sharp Information (310) 379-5179	Helen Burwell B. Enterprises, Inc. (214) 732-0160
<b>CLASSICAL INTELLIGENCE</b>	Rapport Research & Analysis (U.K.) +44 71 355 5020	Aerobureau/STARS (703) SKY-NEWS	OSS. Inc. V: (703) 242-1700 F: (703) 242-1711

**Figure 6: More Intrusive Private Intelligence Capabilities**

**Kroll Associates** (New York) has received favorable publicity as a leader in offering trade secret protection and related private intelligence services. Across the private investigative and "executive services" community, they are the one constant when credible, reliable, international capabilities are discussed.

**Fairfax Group** (Washington, D.C.) provides a range of services from financial investigations of takeover targets to debugging of offices and handling of ransom negotiations for executives.

**Parvus-Jerico** (USA-Bermuda) is run by Jerry Burke, former Executive Director of the President's Foreign Intelligence Advisory Board in the U.S.A., and does especially well in the Caribbean and Latin America.

**Reva Basch.** Author/editor of *Secrets of the Super Searchers*, this lady is widely

regarded as the god-mother of online searchers. A founding member of the Association of Independent Information Producers (AIIP), Reva is respected everywhere--she also has a very strong commitment to ethical guidelines, and believes (and proves every day) that the best private intelligence can be acquired legally and ethically at relatively low cost.

**Seena Sharp** is one of those hard-core New York sharpies transported to California, with a great sense of humor and the ability to do whatever it takes (legally) to get you what you want. She also is one of the founding members of the AIIP.

**Helen Burwell** is the best organized of the independent information brokers, and publishes the *Burwell Directory of Independent Information Brokers*. She knows everyone. knows their strengths and their weaknesses. At my suggestion she recently surveyed all independent brokers for their foreign language and foreign database/resident experiences, and her directory now opens windows into the foreign environment.

Information brokers are very special people. Most companies make the mistake of using a single broker, when in fact there is an entire range of brokers who specialize in very specific areas. Helen's directory is the perfect window into this marvelous global community of very talented people.

In the classical intelligence arena, there are a few people in the Anglo-Saxon community (I am not yet familiar with the Asian and Latin communities) who conduct classical intelligence operations on a for-hire basis. The three I have selected are simply representative.

**Rapport Research & Analysis** has strong roots in the SAS and British intelligence community, and specializes in using ethnic cut-out career agents to securely handle tailored networks in any country. They are also capable of developing rapid-response teams of linguistically qualified interrogators and debriefers who can exploit resident immigrant populations to quickly develop both operational leads and positive intelligence on other countries, organizations, and personalities.

**Aerobureau Corporation** has a very nice air-breathing surveillance aircraft and a program to provide "Strategic Television Airmobile Reports via Satellite" (STARS). The four-engine aircraft includes a remote-controlled drone that can take videos over denied or dangerous areas. Although focused on imagery, they could also be equipped with rapid-response signals equipment, to include fax and telex intercepts.

**OPEN SOURCE SOLUTIONS, Inc.** is an umbrella organization which specializes in knowing who is "best-in-class" for any given requirement at any given time. It provides open sources, systems, and services that are legal, ethical, discreet, responsive, and relatively inexpensive. This can include everything from simple on-line searches to complex telephone surveys, from document acquisition to human network development to real time imagery delivery. The whole point of a clearinghouse is to relieve the customer of the burden of



finding the correct private enterprise intelligence capability, while also "laundering" the customer's requirement by concealing its origin and context, and providing the customer with a quality-control guarantee. Founded originally as a non-profit organization to push U.S. policy, OSS, Inc. has responded to international demand by repositioning itself as a for-profit capable of delivering any open source, system, or service.

### Conclusion

In the information age, "intelligence" is less a matter of penetrating secrets, and more a matter of separating useful information from the flood of open information that is available legally and cheaply, *in order to provide "just in time" decision-support to the consumer.*

In a period of rapidly changing and emerging threats, when fiscal resources for national intelligence are in decline, open sources are proving to be far more capable and responsive than any intelligence analyst would ever have expected, and cost a fraction of their classified counter-part disciplines.

The private sector is a Nation's first line of defense, and also its first line for collection and processing. It is the private sector which offers the cheapest and fastest indications & warning, current intelligence, and even estimative intelligence capabilities.

The concept of "central" intelligence will simply not survive. "National intelligence" must be redefined, and the intelligence community reinvented, in order to harness the distributed intelligence of the Nation, while permitting the intelligence community to conserve its scarce resources. The intelligence community must focus on satisfying a broader range of consumers, on outsourcing collection and analysis to the maximum extent possible, *and on developing clandestine and technical collection capabilities that are truly discreet and able to achieve results without exposure.*

National intelligence communities cannot remain isolated entities relying solely on in-house capabilities funded by the tax-payer. Without a national information strategy, and national vehicles for harnessing the distributed private enterprise intelligence capabilities of the nation (and of other nations), national intelligence communities are at risk of both a 50% cut in their budgets (or worse), and relegation to an obscure role as special action teams restricted to *in extremis* tasking.

The bottom line, however, remains the consumer of intelligence. Today's consumer is sophisticated and constantly exposed to the wide variety of private enterprise intelligence capabilities. Today's consumer is also beset-by fiscal constraints, and it will not take the consumer long to realize that there may be some advantages to "raiding" the intelligence community's budget in order to "distribute" intelligence resources among the consumers themselves. If the intelligence community does not master OSCINT and provide the consumer with a "value-added" contribution in relation to OSCINT, then the day is going to come when the consumer will testify to Parliament that they do not read classified

intelligence, they do not want classified intelligence, or are not willing to pay for classified intelligence. On that day, intelligence as we know it will die.

It is our burden and our privilege to work together to ensure that from the ashes arises a new form of national intelligence, a national intelligence which fully integrates and harnesses the distributed capabilities of each Nation, and serves as the foundation for national security & national competitiveness. Together, in combination, the unclassified capabilities of private enterprise intelligence and those of classified government intelligence can form a "virtual intelligence community" without equal, a virtual intelligence community able to simultaneously inform policy-makers, business, the academy, and citizens.

## APPENDIX B-3

### GLOSSARY

AGSI	Association for Global Strategic Information
AIIP	Association of Independent Information Professionals
ASIDIC	Association of Information and Dissemination Centers
C3I	Command & Control, Communications, and Intelligence
C4I2	C4I and Interoperability
CIA	Central Intelligence Agency
CIM	Corporate Information Management
CIO	Corporate <u>Intelligence</u> Officer (vice Corporate Information Officer)
CNN	Cable News Network
DIA	Defense Intelligence Agency
DMA	Defense Mapping Agency
FBIS	Foreign Broadcast Information Service
FIND/SVP	FIND/S'Il Vous Plait
GII	Global Information Infrastructure
GIM	Global Information Management
HIC	High Intensity Conflict
HUMINT	Human Intelligence (Clandestine, Not Covert or Overt)
IMINT	Imagery Intelligence
K-12	Kindergarten-12th Grade
LIC	Low Intensity Conflict
MASINT	Measurements and Signatures Intelligence
MIC	Mid-Intensity Conflict
NAIC	National Air Intelligence Center
NGIC	National Ground Intelligence Center
NFAIS	National Federation of Abstracting and Information Services
NIF	National Information Foundation
NIJ	National Information Infrastructure
NIM	National Information Management
NMIC	National Maritime Intelligence Center
NRO	National Reconnaissance Office
NSA	National Security Agency
NSF	National Science Foundation
OOTW	Operations Other Than War
OSCINT	Open Source Intelligence (includes imagery and signals)
OSS	Office of Strategic Services
OSS, Inc.	OPEN SOURCE SOLUTIONS, Incorporated
SCIP	Society of Competitor Intelligence Professionals
SIGINT	Signals Intelligence
STARS	Strategic Television Airmobile Reports via Satellite
WAIS	Wide Area Information Service

## APPENDIX B-4

### CORE OPEN SOURCE REFERENCES

NOTE: These are simply a representative sampling. Much of the information is now either in digital form (online, CD-ROM) or published in frequently updated periodicals and directories. *OSS NOTICES* provides monthly notification of new meta-sources.

- Arnold, Steve. *Internet 2000, The Path to the Total Network* (Infonortics, 1994)
- Basch, Reva. *Secrets of the Super Searchers: The Accumulated Wisdom of 23 of the World's Top Online Searchers* (Eight Bit Books, 1993)
- Bernhardt, Douglas. *Perfectly Legal Competitor Intelligence: How to Get It, Use It, and Profit From It* (Financial Times/Pittman Publishing, 1994)
- Bibliography of Business/Competitive and Benchmarking Literature* (Washington Researchers, Ltd. 1994)
- Burwell, Helen. *The Burwell Directory of Information Brokers* (Burwell Enterprises, 1994)
- Coleman, Edwin J. and Ronald A. Morse. *DATA: Where It is and How to Get It: The 1993 Directory of Business, Environment, and Energy Data Sources* (Coleman/Moore Associates, Ltd., 1993)
- Dedijer, Stevan. *A Heteroglossary for Business Intelligence and Security Innovation* (Lund University, August 1993)
- Dedijer, Stevan and Katarina Svensson. *Technical Attaches and Sweden's Innovation Intelligence* (Lund University, April 1994)
- Elias, Arthur W. *The NFAIS Yearbook of the Information Industry: 1993* (Learned Information, Inc., 1993)
- Frey, Donnalyn and Rich Adams. *!%@:: A Directory of Electronic Mail Addressing and Networks* (O'Reilly Associates, 1993)
- From the Top: Profiles of U.S. and Canadian Corporate Libraries and Information Centers* (Special Library Association, 1994)
- Holden-Rhodes, James. *SHARING THE SECRETS: Open Source Intelligence and the War on Drugs* (OSS, Inc., forthcoming)
- Inside Information: Profiles of Association Libraries and Information Centers* (Special Libraries Association, 1994)
- INTERNET PASSPORT: NorthWestNet's Guide to Our World Online (NorthWestNet, 1993)
- Global Perspectives on Competitive Intelligence* (Society of Competitive Intelligence Professionals, 1993)
- Orenstein, Ruth. *Fulltext Sources Online* (Bibliodata, 1994)
- Rosell, Steven S. *et al. Governing in an Information Society* (The Meridian International Institute, date?)
- Rosetto, Louis. *netguide* (1-800-345-8112, 1993)
- Rugge, Sue and Alfred Gloassbrenner. *The Information Broker's Handbook* (Windcrest/McGraw Hill, 1992)
- Tompkins, Alan, *et al. Open Source Intelligence Resources for the Military Intelligence Officer* (434th Military Intelligence Detachment, forthcoming)

## **APPENDIX C**

### **ACCESS:**

#### **Theory and Practice of Intelligence in the Age of Information**

**Robert D. Steele, President  
OPEN SOURCE SOLUTIONS, Inc.**

*95% de l'information dont une entreprise a besoin peut s'acquérir par des moyens honorables.*

*Henry Stiller, Director General  
Histen Riller, Societe Civile*

### **Executive Summary**

- Point #1:** In the Age of Information, "intelligence" is less a matter of penetrating secrets, and more a matter of separating useful information from the flood of open information that is available legally and cheaply: *electronic sources are especially useful.*
- Point #2:** In combination, the economic and political cost of industrial espionage, or penetrations of other governments to divine "plans and intentions", are insupportable when contrasted with the benefits of open source intelligence (OSCINT).
- Point #3:** The concept of "central" intelligence cannot survive in the Age of Information. By focusing on OSCINT, a Nation can mobilize each of its knowledge sectors, and turn the entire Nation into a "virtual" intelligence agency with far greater collection, processing, and action capabilities than are provided by the existing bureaucracies dedicated to national and defense intelligence.
- Point #4:** Comprehensive national knowledge strategies must provide for connectivity, content, culture, coin, and C4 security: the "Five C's".

### **Table of Contents**

**1 Background.** What is the issue; changed "rules of the game"; national information continuum; four information categories; three characteristics of value; speed as the foundation of security; hard copy versus electronic information.

2. Discussion. Role of intelligence and "virtual" intelligence; information as a substitute for capital and labor; possible investment strategy for information; political and economic cost of espionage; pre-publication/pre-secret windows of opportunity; speed advantages of open source exploitation.
3. Information Requirements and Player Identification. Priority versus gaps-driven collection; four major consumer groups of intelligence; refining the gaps-driven requirements process; model for consumer-oriented production; four major target groups for intelligence; four kinds of players in the open source arena.
4. Sources of Information and Methodology. Five distinguishing aspects of information sources; essential reorientation of intelligence toward open sources, privatization of intelligence; five elements of a national knowledge strategy.
5. Industrial Espionage, Sanctions, and Proscribed Information. U.S. views of Japanese and French; general attitudes about industrial espionage; sanctions; proscribed (proprietary) information.
6. Analysis. Rules of the game have changed; competitive advantage has shifted from secrecy to openness; new "order of battle" needed for national intelligence; national knowledge strategy is a critical initiative; strategic opportunity for competitive advantage exists.
7. Action Requirements. Reinvent national intelligence; realign resources; establish a national information requirements council; establish open source focal points within United States and other countries.
8. References. Resume and selected publications; other works of importance; date of information.

# **1. Background**

**What is the issue?** The issue of access has enormous importance for both the national security and the national competitiveness of any Nation.

*The issue for the client is: how does a Nation achieve national security and national competitiveness in the Age of Information, and what does this mean to existing national policies on intelligence organization and the expenditure of public and private funds for information collection, processing, and dissemination activities.*

**Changed "Rules of the Game."** An understanding of the "sources and methods" which comprise "access" in the Age of Information is absolutely vital for top-level decision makers in both government and the private sector. Top-level decision-makers must understand that the "rules of the game" have changed, and that competitive advantage in the

Age of Information is dependent on the laws of cybernetics, not the laws of physics. Under the laws of physics, secrecy and the restriction of knowledge provided a temporary advantage. In cybernetics, openness and flexibility win.

Most great nations spend on the order of \$20 billion to \$30 billion a year on "intelligence", which is traditionally comprised of clandestine human intelligence, and technical collection of imagery and signals.

**National Information Continuum.** At the same time, most great nations have an "information continuum" (illustrated below) whose endeavors and products are going to waste...the capabilities of these elements of the national information continuum are not being exploited! This continuum represents, in a typical great nation, a \$100 billion per year capability that is lying fallow.

K-12	Libraries	PI/IB	Government	Intelligence
<hr/>				
Universities	Business	Media	Defense	

**Figure 1A. The National Information Continuum--Nine Sectors**

NOTE: The above is an original representation that has been current in the literature for over a year. It is different from the more practical Sector Breakout because it reflects a focus on elements of the information continuum which do not--at this time--contribute significantly to national and defense research endeavors.

**Four Information Categories.** There are four "information categories" in the access arena. They are:

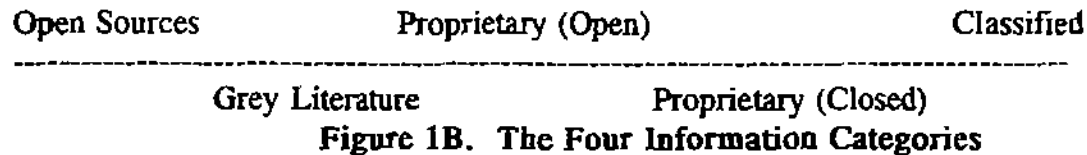
a. Open source or public information: within intelligence communities, this is known as open source intelligence or OSCINT. "Grey literature", literature which is unclassified and not proprietary, but produced in limited quantities for limited purposes, is included as an element of OSCINT. Open (unclassified) electronic information, such as that available through the INTERNET and related file servers and newsgroups, is also included in OSCINT. *The vast majority of scientific & technical intelligence is available through OSCINT, to include 600 scientific & technical journals that appear only in electronic form.*

b. Open proprietary information, discernable through open source investigation. This includes the reverse engineering of legitimately acquired products, and legally conducted "competitor intelligence". (Note: competitor intelligence is the globally accepted term for legal research efforts by businesses studying their competitor's products, organizations, and related matters.)

c. Closed proprietary information, available only through industrial espionage or

clandestine and technical penetrations of regulatory agencies.

d. Classified information, available only through clandestine human intelligence or technical (imagery or signals) intelligence.



**Three Characteristics of Value.** The value of information is derived from three characteristics of the information: its substance or content; the context within which it is being considered by others; and the timing with which it is received.

*The single most significant step an organization can take to increase the value of the information it is acquiring is to increase the speed with which the information is acquired and acted upon. This is also the most inexpensive step-but only if top management is willing to accept significant changes in doctrine and procedure.*

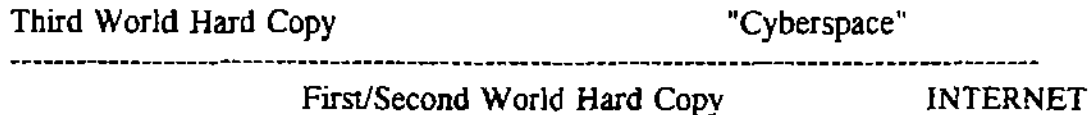
**Speed as the Foundation for Security.** The speed with which information moves and achieves value depends less on the information itself (the externality) and more on the degree to which the participating organizations are organized and aware of their requirements (the internality). Organizations are drowning in information because they have not learned to swim. They are not trained, equipped, or organized to collect, process, disseminate, and act upon information. The most important employees, the ones with the contextual understanding of the situation, are normally not empowered to act on information, and normally do not receive intelligence products.

Imbuing a national infrastructure with "speed" really means that a complete change is required in the way in which organizations relate to one another, and in the way in which managers relate to front line workers or action officers. The beauty of working with open sources is that it eliminates, in a single stroke, all of the political and legal, as well as the economic, constraints that characterize the sharing of classified information. We have been trying to water the desert with oil, instead of water.

**Hard Copy versus Electronic Information.** Finally, in discussing issues of access, it is important to understand the relative value of hard copy versus electronic information. Although hard-copy information far outweighs electronic sources in quantity, and particularly in relation to Third World sources, the electronic world is where "up and coming" technologists as well as "up and coming" leaders are communicating their most significant thoughts.



*The electronic world is especially useful because it allows an enormous amount of research to be conducted from a single location, and also allows relatively anonymous browsing through other computers or commercially available databases. Hard-copy is an important secondary source, especially when investigating Third World and non-technical issues.*



**Figure 1C. Hard Copy versus Electronic Information**

## 2. Discussion

**Role of Intelligence and "Virtual" Intelligence.** There is no issue more important to a Nation in the Age of Information than that of the role of intelligence--not only of the role of the traditional national intelligence services, but also of the non-traditional "virtual" intelligence services which are represented by the other elements of the national information continuum.

*A proper perspective on this matter, at the highest levels of both the government and the private sector, represents at least a \$100 billion a year value. This is enormously important, not only because it will be the major policy area affecting the future of the Nation, but because it is relatively easy to achieve by realigning and coordinating existing capabilities and funds.*

**Information as a Substitute for Capital and Labor.** In the Age of Information, when information is the "first order" commodity, and information is a substitute for time, space, capital, and labor, the implications of this discussion are enormous. The fate of the Nation depends on a proper appreciation of this issue, and on adequate coordination between government and private sector leaders responsible for elements of the information continuum.

**Possible Investment Strategy for Information.** The four "information categories" in the access arena can be evaluated as follows:

-- Open source: 80% of what is required for sound decision-making, at 20% of the cost, in 20% of the time (relative to industrial espionage or classified collection). The value of open source information cannot be exaggerated.

-- Proprietary (open): 5% of what is required, for an additional 10% cost increment.

-- Proprietary (closed): 5% of what is required, for an additional 20% cost increment.

-- Classified: 10% of what is required, for an additional 50% cost increment.

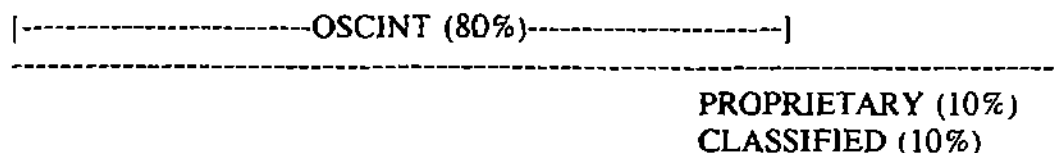


Figure 2A. Possible Investment Strategy for Information

**Political and Economic Cost of Espionage.** It merits comment that industrial espionage in particular, but clandestine and technical intelligence as well, reflects a political risk, or a potential political cost, that is easily triple the economic cost--industrial espionage and classified penetrations are not only twice as costly as open source exploitation, they are also twice as likely to "explode" in the face of their sponsor.

**Pre-Publication/Pre-Secret Windows of Opportunity.** In the area of open source information, or open source intelligence (OSCINT), it is very important that decision-makers understand the levels of access in terms of time  
--time is the vital aspect of cybernetics, and is the critical factor in national competitiveness:

Published sources are available to mass audiences at the same time--books are generally provided to the public years after they were actually written; articles generally months after they were written; and newspaper reporting days or weeks after being drafted..

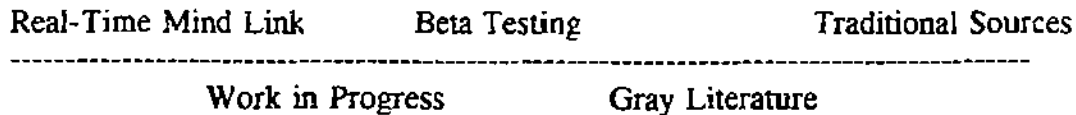
"Grey literature" is available to specialized audiences at the same time, and to non-members after a period of time.

"Work in progress" is available to peer review groups and to specially equipped "outsiders".

"Pre-publication intelligence" is available to specially equipped outsiders who take the trouble to identify and cultivate selected sources of public information. This area is the "center of gravity" for those who seek to "reinvent" national intelligence.

**Speed Advantages of Open Source Exploitation.** There are two reasons why open source intelligence (OSCINT) is a vital area of concentration: the first is that most applied technology, including proprietary or classified technology, begins with open publications about its sub-elements, and it is often possible to piece together very good intelligence reports "at the source" while avoiding the risk of industrial espionage or clandestine operations against foreign targets. The second reason is that every "dual-use" technology to which export controls are eventually applied spends at least two years, and sometimes up to ten years, in "beta" development. The Department of Commerce, which has the lead in classifying dual-use technology, is generally two years behind actual market developments; this is particularly true in the software arena. Thus, the best time to capture a "secret" or a restricted technology, is during the two year "beta" window before it becomes a secret or is

restricted.



**Figure 2B. Speed Advantages in Open Source Exploitation**

Refining one's open source intelligence (OSCINT) intelligence process to collect information in the pre-publication stage, by identifying and keeping in touch with key experts who provide advance looks at "works in progress", adds a further six months to a year of competitive advantage. *Electronic searching is the single most vital tool in identifying these experts "in time".*

### **3. Information Requirements and Player Identification**

There are three ways of looking at the information playing field: by focusing on the four consumer groups for national intelligence; by focusing on the four warrior classes of the future; and by focusing on the sources of information. Each will be discussed in turn, together with a means of executing gaps-driven collection and consumer-oriented production.

**Priority versus Gaps-Driven Collection.** The information requirements arena is traditionally one which intelligence communities have not mastered. Too often they collect what is collectable, or obviously protected, and they rarely produce intelligence that is tailored to a specific customer or delivered "just in time". Information requirements are typically driven by gross priorities (e.g. the Soviets are priority one, the Chinese priority two), rather than by "gaps" or real requirements. This often means that Third World encyclopedic intelligence (most of which is unclassified), and economic or demographic intelligence vital to penetrating foreign markets, does not receive the attention it requires.

**Four Major Consumer Groups of Intelligence.** There are four specific groups of information customers that every intelligence organization should be serving, but generally does not, because it focuses on the very highest levels of government rather than on the subordinate levels where policy is actually created and actions are taken on a day to day basis.

a. Departmental planners and programmers, in every Department of government, not only in the national security arena, require both strategic generalizations (rather than a flood of detailed reports about tiny parts of many problems), and political-military information heavily laden with information about "plans and intentions".

b. Regional planners and programmers, including Ambassadors and Assistant Secretaries of every Department of government, require regional generalizations and very detailed mobility and market information. This is the customer group most likely to take

advantage of intelligence which focuses on opportunities for advantage, opportunities to prevent disaster or establish commercial gains before anyone else realizes there is a threat or an opportunity to be contested.

c. Ambassadors and corporate general managers in specific countries require both detail about the physical capabilities of their opponents or competitors, and very detailed evaluations of sustainability, availability, reliability, and or accuracy of competitor products. In the economic arena, intelligence about demographics and culture is more easily obtained, and more valuable, than internal corporate information about competing products. If you understand the BUYER's requirements, you do not need to collect every detail about competing SELLER's capabilities. This point merits elaboration: competitive advantage comes from satisfying the buyer, not from beating the opposing seller. It is far more important to understand every detail about what the buyer wants to buy, than attempting to understand opposing solutions.

d. System designers and project managers, and those at the most senior levels who make acquisition and investment decisions, generally receive adequate intelligence about technical details, but do not receive good intelligence (intelligence which is generally unclassified) about whether the system is really worth acquiring in terms of cost-value, competing means of meeting the requirement, cost of sustainability, and so on. For instance, most advanced nations have invested billions of dollars in fast-moving sophisticated systems and failed to establish the necessary communications and computer support to actually make those systems effective in the field.

System Designers

Regional Planners

-----  
General Managers

Department Planners

**Figure 3A. Four Major Consumer Groups for Intelligence**

**Refining the Gaps-Driven Requirements Process.** The greatest flaw in a priority-driven requirements process is that it is divorced from the day to day needs of the policy and action-level consumer. Priority-driven collection tends to err on the side of repetitive and "vacuum cleaner" collection against the highest priorities, and to completely disregard both encyclopedic and current intelligence requirements for targets which may be of a lesser priority in the "grand strategy" arena, but of vital interest at the operational and tactical levels. A gap-driven information requirements process will take its requirements each day (rather than through monthly or quarterly "priorities validation" meetings), both from the consumer of intelligence ("here is what I need to know tomorrow") and from the analyst ("here are the things I did not know in producing this report").

**Model for Consumer-Oriented Production.** The existing production model, at least in the United States, is based on "stove-pipe" production which is rarely as "all-source" as it could be (e.g. the National Security Agency produces reports drawn largely from signals

intelligence). and is also severely deficient because it focuses on specific countries, topics, or weapons systems--i.e. the production is defined by the target, not by the needs of the consumer. Below is illustrated a superior line of consumer-oriented products, most of which would be unclassified and whose contents would be primarily drawn from open sources of intelligence.

**BASIC PRODUCTION: COUNTRY PROFILES.** Integrate executive summaries for each of the four consumer groups, with brief encyclopedic intelligence summaries of each of the key industrial, geographic, and civil factors.

**STRATEGIC PRODUCTION.** Tailored products that focus on establishing *strategic generalizations* pertinent to specific mission areas (e.g. aircraft, automobiles, textiles), specific regions, and specific timeframes (generally long-term).

**OPERATIONAL PRODUCTION.** Tailored products focused on *regional generalizations* with a special emphasis on industrial areas within the region, on seasonal differences (whether terrain or trade), and on leadership character and demographics.

**TACTICAL PRODUCTION..** For each industrial area (or industry area) both generalizations and specifics country by country, with emphasis on terrain, climatic, and civil constraints. It is only at this level that a consumer should have to deal with the level of detail which now characterizes most intelligence community products.

**TECHNICAL PRODUCTION.** Get away from system-specific production, and move instead toward industry-area production with regional and timeframe sub-sets. Focus on support to cost-benefit and trade-off decisions, not on the system in isolation.

### **Figure 3B. Model for Consumer-Oriented Production**

**Four Major Target Groups for Intelligence.** There are four specific targets for information and intelligence activities; each of these target groups must be completely understood if a Nation is to maintain both its national security and its national competitiveness. Each target group has a different source of power, and a different way of training, organizing, and equipping itself for battle. Each requires a different intelligence approach and in essence a different kind of intelligence community. The traditional intelligence officer will not be competent against all four of the target sets--four different kinds of intelligence organizations must be trained, equipped, and organized for their specific target set.

a. The High-Tech Brute, similar to the United States of America, is that group which relies on expensive technical capabilities and huge logistics trains. In industrial terms, this is the capital-intensive player.

b. The Low-Tech Brute, such as the narcotics trafficker or the Italian crime family, represents a "needle in the haystack" problem. In industrial terms, this is the labor-intensive player.

c. The High-Tech Seer, such as highly skilled and knowledgeable computer engineers, is comprised of both conglomerations of skilled individuals engaging in economic warfare, and single individuals, "hackers", able to penetrate advanced computer and telecommunications networks. In industrial terms, this is the brain-intensive player.

d. The Low-Tech Seer, such as the Islamic Fundamentalists, or Asian gangs in the United States, are those whose "weapons" are of a cultural or demographic kind, whose "command and control" system is comprised of the television and the pulpit--very difficult for a Western intelligence service to understand and address. In industrial terms, this is the labor union.

*In each of these cases, using electronic sources of news and information provides a significant competitive advantage in terms of time, scope of review, and depth of understanding.*



**Figure 3C. Four Major Target Groups for Intelligence**

**Four Kinds of Players in the Open Source Arena.** The diagram in the "Background" section clearly identified the nine constituencies in the access arena. Naturally there are sub-constituencies (e.g. government is divided at the federal level into legislative, executive, and judicial, and also into federal, state, and local; media is divided into mainstream national papers, regional papers, niche journals, and technical newsletters).

In general terms, there are four kinds of players:

-- Those who talk to one another but are not influential, are divorced from practical military or commercial applications: the "ivory tower" academics. Spend 10% of your resources on this group.

-- Those who are influential but do not quote one another and contribute nothing substantial: the "bandwagon" journalists. Spend 10% of your resources on this group.

-- Those who are both connected to one another and influential--this constitutes the "mainstream" of current thinking. The downside of the mainstream is that it tends to reflect conventional wisdom rather than innovative or revolutionary thinking. Spend 20% on this group.

-- Those--and they are a small group--that are neither connected nor influential, but who are in fact the "up and coming" leaders in their disciplines. It is this group which not only represents the greatest potential value for a Nation, but which is the least protected! The only obstacle to exploiting this group is internal, it is bureaucratic! Spend 60% on this group. Although intelligence organizations are accustomed to thinking of this group as a source of "sleeper" agents, in fact it should be thought of as a source of "avant garde" thinking which is not only of enormous importance to international competitiveness and domestic security, but predominantly unclassified.

Mainstream (20%)	Up and Coming (60%)
Bandwagon (10%)	Ivory Tower (10%)

Figure 3D. Four Kinds of Players in the Open Source Arena

#### 4. Sources of Information and Methodology

Five Distinguishing Aspects of Information Sources. Sources of information can be classified by medium, location, discipline, language, and level of classification.

The most pervasive medium is hard-copy information. However, most of the hard-copy information is of relatively low grade, and often not worth the expense of acquisition. Never-the-less, it cannot be ignored. Spend 20% of your resources on the hard-copy medium.

The next major medium is micro-fiche; although many organizations are phasing out their micro-fiche holdings, this remains an important medium, particularly in the patent and archival worlds. Spend 10% on this medium.

Electronic information is available through online services as well as offline products. It is important to emphasize that electronic information includes imagery (SPOT, LANDSAT) as well as signals (foreign radio and television broadcasts, unencrypted cellular telephones, facsimiles, and telex transmissions). It is also important to note that, despite the fact that electronic information is a relatively small arena of interest in relation to hard-copy and microfiche, it is "exploding" and already dominates many of the most advanced disciplines as the "medium of choice. For instance, this medium contains over 600 scientific journals online that do not appear in hard-copy at all. *The electronic medium is the battleground where strategic advantage can be gained at relatively low cost and with no political risk--it is open, it is pervasive, and it is not being exploited by other countries as well as it could be--*

*this is a very important area. Spend 40% of your resources on this medium.*

The most subtle storage medium is the human brain. No intelligence service will ever master the data entry or data collection problem. The most important capability any intelligence service can develop is that of establishing real-time mind-links between the customer and the best available source. The "intelligence minuteman" concept, first articulated in December 1992 at the First International Symposium on "National Security & National Competitiveness: Open Source Solutions", is the wave of the future. Spend 30% of your resources on this medium. Note that this medium provides real-time access to the other mediums--the human expert responsive to tasking can rapidly collect, process, and disseminate essential information from the other mediums, on demand.

It is important to note that in the Age of Information technology has made possible a radical shift in why and when one acquires information. It is now possible to train, equip, and organize collectors of information for "just in time" collection instead of "just in case" collection. Hard copy and microfiche were the dominant storage mediums under the old "just in case" paradigm. Electronic information, and direct access to an enormous global pool of over human assets are the dominant access mechanisms under the new paradigm.

The location of the information is both geographic and physical. Some information cannot be obtained without a personal visit to its location. Most information can be obtained remotely, through a telephone call or correspondence, and payment if necessary to the appropriate person.

*A single researcher skilled at remote data acquisition for a particular region is more valuable than 100 clandestine case officers spread over ten countries. Physically the information might be part of a central filing system or a personal filing system. 80% of the time the information will be part of a personal filing system, which reiterates the critical importance of developing human paths to the information.*

Professional disciplines (e.g. physics, electro-optics) are the most global and well-organized structures through which to acquire information. Penetrating a professional association with global links is far more useful than penetrating a single government's nuclear facility, to take one example. Again, professional associations provide the human links and paths toward virtually any information--they are also the most likely to publish information before it becomes classified. It is futile to train intelligence professionals to pretend to be scientists. It is much more useful and cost-effective to provide existing scientists with the finest communication tools and travel budgets possible--they will absorb far more, and be able to report far more, than a few case officers working with a few agents of limited access.

Language skills cannot be ignored. English, French, Spanish, Japanese, Chinese, and Arabic are the most important languages, followed by Russian, Punjabi, Hindu, and Hebrew. Any international intelligence or information service which does not have at least 100 people



fluent in each of the most important languages, and at least 20 people fluent in each of the minor languages listed above, is not serious. Language translation programs (e.g. Global Link) are important aids, and can be used to reduce the time of translation for a typical document from eight hours to three. The importance of linguistic and cultural nuances should not be underestimated. The language of the consumer should be the language of production, even if this involves extraordinary cost.

Level of classification (in governments generally Confidential, Secret, Top Secret, and Codeword; in business generally Proprietary, Trade Secret, Executive Only) is the most misunderstood and over-rated basis for selecting information. Enormous amounts of money are wasted, and significant political risk is undertaken, to obtain information that is classified "secret" or "proprietary". This is a fundamental mistake which reflects a lack of understanding about how knowledge works in society, a lack of understanding of current trends in information sources and methods.

MEDIUM	DISCIPLINE	CLASSIFICATION
-----	-----	-----
LOCATION	LANGUAGE	

**Figure 4A. Five Distinguishing Aspects of Information Sources**

**Essential Reorientation of Intelligence Toward Open Sources.** The methods used to obtain information should be appropriate to the sector of information generation that is being studied. Each of the nine sectors has information producers. Each nation has representatives of their own in sectors of their own. For instance, your own journalists are frequently the best means of approaching foreign journalists, and of monitoring the production and the human sources being used by foreign journalists.

The fundamental flaw in the "methods" of most intelligence agencies is that they attempt to acquire all information using their own personnel and clandestine or technical methods. Instead, they should leverage the other sectors of the information continuum, and establish a "virtual" intelligence community that is comprehensive. By focusing on open information and the open exploitation of individuals in all sectors, a Nation with a \$10 billion intelligence budget can leverage another \$90 billion in existing independent but exploitable "virtual" intelligence capabilities whose "overhead" costs are not being paid by the government. The electronic medium is the "lever that can move the world" and give the intelligence professional enormous access.

#### **Privatization of Intelligence**

*The most fundamental change in "methods", besides moving away from investments in clandestine and technical intelligence capabilities, and toward investments in open source intelligence, is that of the privatization of intelligence. It is more efficient, most cost-effective, indeed, more discreet, to*

*utilize ad hoc private collectors and processors of information, than it is to use existing bureaucracies, including existing intelligence agencies and existing Embassies or local corporate offices overseas.*

**Five Elements of a National Knowledge Strategy.** This focus on openness is extremely important because it means that the fruits of this open source intelligence effort can be shared directly with industry, the press, and the legislature, without the slightest political risk. For those who do not understand how "open" information can provide a competitive advantage, consider only how disorganized everyone else is--the first Nation to establish a national knowledge strategy which harnesses the full power of their information continuum will achieve an enormous competitive advantage as we enter the Age of Information. A national knowledge strategy is comprised for five elements:

a. **CONNECTIVITY.** Provide leading representatives within each sector with the telecomputing tools they require to keep in touch with their counterparts in all other countries, and with one another. At the same time, provide government and corporate intelligence analysts with the same tools, and provide everyone with incentives to communicate with one another.

b. **CONTENT.** Provide incentives to all parties to maximize the amount of information that they put "online"; the government can increase online information by testing new economic models (for instance, the "compound interest" model instead of the "single sale" model for compensating authors) and making appropriate adjustments to copyright and patent law. This is a two-way concept. It is not only important to increase the amount of foreign language material that is captured, translated, and placed online, but it is equally important that great emphasis be placed on exporting national intellectual products which have been fully and accurately translated into major foreign languages such as English, Japanese, and Chinese. In the Age of Information, "gunboat diplomacy" has been replaced by intellectual influence. The quality of a nation's intellectual output, and the degree to which it is made useable by others, will have a dramatic impact on the strategic position of the Nation.

c. **CULTURE.** Recognize the importance of accelerating the integration of ethnic populations and economically impoverished citizens. In particular, those ethnic groups which speak and read fluently the language of their adopted country, and the language of their former country, are priceless national assets which can be used as interpreters and translators.

d. **COIN.** A typical major nation wastes on the order of \$2 billion a year just on end-user fiddling with personal computer hardware and software combinations. If all redundant and contradictory research & development were brought under control, just in the information technology arena, a typical major nation would probably save on the order of \$10-20 billion a year.

e. **C4 SECURITY.** Every nation, and particularly the advanced nations of Europe

and the Anglo-Saxon world, is extremely vulnerable to the interruption of command & control, communications, and computing services.

Virtually every major antenna system, including the downlinks from the satellites, is completely unprotected. No nation has established a serious C4 security posture that recognized the degree to which government, military, and economic communications depend on a very vulnerable civil infrastructure. No nation has established an effective "cyberspace order of battle". This is the "Pearl Harbor" of the Age of Information, waiting to happen.

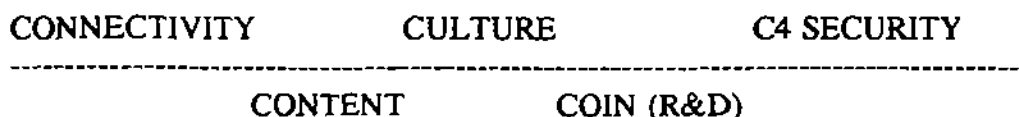


Figure 4B. The Five Elements of a National Knowledge Strategy

#### 5. Industrial Espionage, Sanctions, and Proscribed Information

U.S. Views of Japanese and French. There is a very strong perception within the United States that the Japanese view economic competition as "war", and that the French, while not necessarily viewing economic competition as war, are willing to engage in "unethical" measures including direct support from government intelligence agencies to specific French companies. The book Friendly Spies: How America's Allies are Using Economic Espionage to Steal Our Secrets, while discredited in some circles, has done enormous damage to French interests in the U.S. The running joke about Air France seats being "bugged", very common in U.S. business circles, is a good sign of how deeply this book has penetrated the "psyche" of the U.S. business community.

General Attitudes About Industrial Espionage. Most U.S. companies do not have a full appreciation of how easily others can penetrate their organizations, and most do not engage in significant industrial espionage. For instance, most U.S. companies have absolutely no computer security and no measures to protect their computers from external penetration. They are completely unaware of the ease with which computer screens and computer emissions can be captured from a van parked outside their building. There is a general sense among U.S. firms that industrial espionage is "not worth it". There are two exceptions to this: the first is the hiring of executives and key employees from competitor firms, and the second is bribery, but only overseas.

Sanctions. The Toshiba case is a good example of the sanctions that might be imposed in specific instances when there is a public knowledge of violation, but in general the U.S. government will not publicize or act on cases of industrial espionage.

Proscribed (Proprietary) Information. There is a strong trend in the United States toward openness. This is true of the government, where many "secrets" and many secret technologies are about to be declassified, and also of industry, where there is a growing understanding that the restriction of information imposes internal costs that may not be

warranted. In the case of specific chemical formulas or other "protectable" secrets, this may not be so, but in the case of general engineering practices, targeted markets, and so on, the general focus is on openness and staying ahead of the competition, rather than on protecting secrets.

## 6. Analysis

The client is better able to evaluate the applicability of this new theory and practice of intelligence to their needs, but on balance one must conclude:

**"Rules of the Game" Have Changed.** The Age of Information has redefined our concepts of war and peace, of national security and national competitiveness. The "rules of the game" have changed, and there has been a reordering of both power and the sources of power. Information is now a commodity, and the most important resource to any Nation.

**Competitive Advantage Has Shifted From Secrecy to Openness.** The Age of Information has destroyed the ability of individuals, organizations, and governments to control information or restrict the dissemination of information. It is virtually impossible to keep a "secret" in this day and age. Hence, the competitive advantage has shifted from those able to conduct research in secret, to those able to RAPIDLY exploit the efforts of others through openly available information collected "just in time".

**New "Order of Battle" Needed for National Intelligence.** The Age of Information requires a new "order of battle" philosophy within national governments and their major corporate sectors. The degree to which individual minds can be linked across sectors now becomes more important than the number of tanks one has--existing conventional forces can be immobilized, and existing industrial processes can be superceded, by relatively modest applications of knowledge. *The rapid development of competent electronic search & retrieval specialists, and particularly specialists in scientific & technical databases and newsgroups, as well as cultural matters, should be a national priority.*

**National Knowledge Strategy is a Critical Initiative.** Although there are several nations, including Japan, Sweden, Israel, and Taiwan (and their tribal villages world-wide) which are generally ahead of all others in their national knowledge activities, no nation has actually developed a national knowledge strategy nor harnessed the potential of its nine sectors in the information continuum--a continuum that constitute a "virtual" intelligence community of enormous power.

**Strategic Opportunity for Competitive Advantage Exists.** A strategic opportunity for competitive advantage exists. In my judgement there is about a two to five year window within which an organized national effort can reap enormous dividends. After that time many organizations will both realize the power of open information and start developing their own collection capabilities more fully, and public encryption will be widespread, introducing a "Tower of Babel" effect into the "electronic English" information commons that is just

beginning to appear.

## 7. Action Requirements

a. **Reinvent National Intelligence.** Each nation has an enormous store of non-traditional intelligence and information capabilities outside of government that are rarely called upon. Consider the potential of these non-traditional sources, and develop plans for the total mobilization of the nation's intellectual power.

b. **Realign Resources.** Roughly 80% of the existing intelligence budget could be realigned to open source intelligence (OSCINT) collection, processing, and dissemination, in close cooperation with the other elements of the national information continuum, who might be inspired to effect their own realignments once they see the government in a leadership role.

CLASSIFIED INTELLIGENCE		10%
PROPRIETARY INTELLIGENCE		10%
OPEN SOURCE INTELLIGENCE		80%
Human Sources	30%	24%
-- "Up and Coming"	60%	24%
-- Mainstream	20%	08%
-- Bandwagon	10%	04%
-- Ivory Tower	10%	04%
Hard Copy	20%	16%
Microfiche	10%	08%
Electronic	40%	32%

NOTE: Column one percentages are 100% of subheading percentage in column two, while column two percentages are 100% of column three subheading. The percentages in column three are actual percentages of the total budget.

**Figure 7A. Notional National Intelligence Resource Realignments**

c. **Establish a National Information Requirements Council.** Identify an organization able to coordinate demands for information with global collection activities and impose the common sense guideline of exploiting open sources as "the source of first resort". This has the interesting ramification of also making much more of what we need to know obtainable through private sector capabilities rather than government capabilities.

**d. Establish Open Source Focal Points Within United States and Other Countries.** Within the United States, contract with two separate organizations: the first should serve as a complement to the Embassy and as a rapid-response local representative for the national intelligence council. Its role should be one of requirements management, oversight, and product packaging. The second organization should actually carry out all the research through sub-contracted collection and production, with value-added quality control. Similar arrangements can be made in other countries, perhaps by building on the established SVP network.

## **8. References**

A resume and a list of selected personal publications are attached. The *Proceedings* of the First International Symposium on "National Security & National Competitiveness: Open Source Solutions", are the sole existing foundation for a national intelligence restructuring of this magnitude. A copy of both volumes is provided as part of this report, together with copies of more recent articles, speeches, and testimony bearing on this issue.

Other works of importance include: Jon Sigurdson and Yael Tagerud (eds), *The Intelligent Corporation: The Privatization of Intelligence* (Taylor Graham, 1992); Alvin Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century* (Little, Brown, forthcoming), see especially the chapters on knowledge warriors and the future of the spy. Winn Schwartau, *Information Warfare: How to Wage and Win War in Cyberspace* (Interpact, forthcoming); James Holden-Rhodes, *Sharing the Secrets: Open Source Intelligence and the War on Drugs* (Sandia National Laboratory, forthcoming)

**9. Date of Information.** 17 September 1993

## APPENDIX D

### CONCISE DIRECTORY OF SELECTED INTERNATIONAL OPEN SOURCES & SERVICES

DOI: 1 March 1996

Prepared by Robert D. Steele

Based on Research As Published in *OSS NOTICES* 1992-1996

#### ACCESS INNOVATIONS, INC.

Ms. Marjorie Hlava, President  
Post Office Box 40130  
Albuquerque, NM 87196  
Voice: (505) 265-3591  
Fax: (505) 256-1080

Ms. Hlava has been past president of the major information associations in the USA including the American Society for Information Science and the Association of Independent Information Producers.

#### BDM FEDERAL

Mr. Tom Price III  
Principal Staff Member  
1501 BDM Way  
McLean, VA 22101-3204  
Voice: (703) 848-5203  
Fax: (703) 848-6683

The National Security & Technology Applications Division is under the leadership of LtGen C. Norman Wood, USAF (Ret), former Director of the Intelligence Community Staff, and specialized in OSINT support to U.S. intelligence.

#### BRITISH LIBRARY, THE

Mr. Mike Curston  
Document Supply Centre  
Boston Spa, Wetherby  
West yorkshire LS23 7BQ  
UNITED KINGDOM  
Voice: (44 937) 546-333  
Fax: (44 937) 546-061

Something like the U.S. Library of Congress, but better organized and focused on solid business practices. Known world-wide for its access to obscure sources and especially for its access to conference proceedings. Produces CD-ROMS, others aids.

#### BURWELL ENTERPRISES

Ms. Joanne Pauline  
Marketing Director  
3724 FM 1960W, Suite 214  
Houston, TX 77068  
Voice: (713) 486-3500 x 2353  
Fax: (713) 920-7086

Ms. Helen Burwell is the publisher of the *Burwell Directory of International Information Brokers*, and recently added an index to this work which identifies brokers who speak a foreign language, and are familiar with in-country databases.

#### CIESIN (CONSORTIUM FOR INTERNATIONAL EARTH SCIENCE NETWORK)

Mr. Robert J. Coullahan

Director of Government & International Programs  
1747 Pennsylvania Avenue, N.W.  
Suite 200  
Washington, D.C. 20006  
Voice: (202) 775-6606  
Fax: (202) 775-6622

This organization is a non-profit and one of the best sources of meta-data: data about environmental information, including imagery and seismic data, held by others around the world. Excellent advisors.

## **CISTI**

The Canada Institute for Scientific and Technical Information, originally focused on meeting the needs of Canada, has expanded in recent years to offer its services to the North American customer base. Their online catalogue is available free at <http://www.cisti.nrc.ca/cisti/serlist.html>. For more information contact Document Delivery Services, CISTI, National Research Council, Ottawa, Ontario K1A 0S2, Canada. Voice: (613) 993-9251, facsimile (613) 952-8243. Email: [cisti.docdel@nrc.ca](mailto:cisti.docdel@nrc.ca).

## **CLEARINGHOUSE FOR SUBJECT-ORIENTED INTERNET RESOURCES**

University of Michigan

60 subject-matter guides including:

Aerospace Engineering

Archives on the Internet

Government Sources of Business & Economic Information

Neurosciences Internet Resource Guide

U.S. technology Public Policy

Example of university resources being applied for the common good.

[gopher.lib.umich.edu](http://gopher.lib.umich.edu). look for "What's New and Featured resources", go to "Clearinghouse". Or anonymous ftp to [una.hh.lib.umich.edu path:/inetdirstaks](ftp://una.hh.lib.umich.edu/path:/inetdirstaks). If you have trouble, email [lou@umich.edu](mailto:lou@umich.edu).

## **Derwent World Patents Index**

Available through DIALOG, Questel/Orbit, and STN. Communicate with Derwent Publications, Ltd., Derwent House, 14 Great Queen Street, London WC2B 5DF, United Kingdom. Voice: (44 171) 344-2800 or in the USA (703) 790-0400. Web: <http://193.128.218.44/products/>.

## **DIALOG (Knight-Ridder)**

Mr. David Brown, Team Leader  
Government Team, Suite 500  
1901 North Moore Street  
Arlington, VA 22209  
Voice: (703) 908-2383  
Fax: (703) 524-1680

One of the two leading commercial online services--it is very important to understand that both DIALOG and LEXIS-NEXIS are required to "hit" 2/5ths of the available online information, and that the other 3/5ths require additional research.



### ***Directory of Publications and Broadcast Media***

Available from Gale Research for \$295. ISBN 0-8103-7188X. Formerly titled the *Directory of Directories*, this is a recommended starting point for virtually any search.

#### **Disclosure, Inc.**

Disclosure, Inc., 5161 River Road, Building 60, Bethesda, MD 20816. Web:  
<<http://www.disclosure.com/>>.

#### **E2G (UK)**

Mr. William Owen, Managing Director  
2nd Floor, 1 Northumberland Avenue  
Trafalgar Square  
London WC2 N5BW ENGLAND  
Voice: (44 171) 487-3626  
Fax: (44 171) 487-3817

Former Special Air Service and other British special forces personnel are available through this organization to conduct route reconnaissance, develop military maps, and provide other pre-landing support services.

#### **EASTVIEW PUBLICATIONS**

Manager  
Gray Literature Acquisitions  
3020 Harbor Lane N  
Minneapolis, MN 55447  
Voice: (612) 500-0961  
Fax: (612) 559-2931

This organization is one of the best in the world at acquiring "grey literature", with a strong specialization in Russian and East European literature. They are also the foremost source of Third World maps, including tactical maps, created by USSR.

### ***Encyclopedia of Associations***

Available from Gale Research for \$250. ISBN 0-8103-7421-8.

#### ***FIND IT FAST: HOW TO UNCOVER EXPERT INFORMATION ON ANY SUBJECT***

Robert Beckman, Author  
Harper Collins, Publisher  
\$13, Cost  
(800) 427-7372

As described--an essential handbook for the analyst interested in exploiting the open source world.

#### **FIND/SVP**

Mr. Joseph Cositore, Vice President  
625 Avenue of the Americas  
New York City, NY 10011-2002  
Voice: (212) 645-4500  
Fax: (212) 645-7681

FIND/SVP ("SVP" in French stands for "if you please") specializes in obtaining any article, any document, through a world-wide network of franchises. It does almost no analysis, just acquisition.

## **FULD & COMPANY**

Mr. Leonard Fuld, President  
80 Trowbridge Street  
Cambridge, MA 02138  
Voice: (617) 492-5900  
Fax: (617) 492-7108

Publisher of *The New Competitor Intelligence*, a handbook for business intelligence specialists. Includes resource listing--strongest of Europe.

## **GaleNet**

GaleNet can be used by anyone with an Internet connection, either dial-up or direct, and a graphical World-Wide-Web browser. The Web site offers a demonstration area. OSS tested their site by accessing the *Encyclopedia of Associations*, using the word "information", and found 138 associations that have "information" in the keyword search field. To arrange for a demonstration of GaleNet at your site, or for more information, please call the National Field Sales Manager, Mr. Tim Brandner, at (510) 671-5379, or send email to <Tim\_brandner@gale.com>.

## **Genuine Article**

A service of the Institute of Scientific Information. Contact Mr. Frank Spiecker, 3501 Market Street, Philadelphia, PA 19104. Voice: (215) 386-0100 extension 1374; Facsimile: (215) 386) 6362. Web: <<http://www.isinet.com/>>.

## **GUIDE TO NETWORK RESOURCE TOOLS**

by European Academic & Research Network                      As described.  
Free of charge online  
Go to <[listserv@earncc.bitnet](mailto:listserv@earncc.bitnet)>  
Send command <GET NETTOOLS PS> (for postscript) or  
Send command <GET NETTOOLS MEMO> (for plaintext)  
Covers Archie, Astra, Bittip, Gopher, Listserv, Netnews, Netserv,  
Trickle, WAIS, Whois, and World-Wide-Web

## **INDIVIDUAL, INC.**

Director, New Business  
8 New England Executive Park West  
Burlington, MA 01803  
Voice: (617) 273-6000  
Fax: (617) 273-6060

This is one of the finest "current awareness" services, providing a one page listing of "hits" on your profile by fax or email, with full-text available immediately through automated order.

## **Information Broker's Handbook**

By Sue Rugge and Alfred Glossbrenner. Published by Windcrest/McGraw-Hill, 1992. ISBN 0-8306-3797-4. \$30.95, order through local bookstores.

## **INFOSOUTH**

University of Miami  
(800) 752-9567

Translations of Latin American press.  
biographies on Latin American leaders.

## **INSIDE INFORMATION: PROFILES OF ASSOCIATION LIBRARIES AND INFORMATION CENTERS**

**Special Libraries Association**  
Mr. Kevin Heffner, Director  
Fund Development  
1700 Eighteenth Street, N.W.  
Washington, D.C. 20009  
Voice: (202) 234-4700 ext. 631  
Fax: (202) 265-9317

This is the international organization that serves over 15,000 librarians in charge of small specialized libraries for associations, corporations, or other special interests. This is an essential networking vehicle for reaching limited edition publications, especially in economic and financial arena.

## **International Thomson Publishing**

Their Web site is located at <<http://www.thomson.com>>. To receive a catalog you can write to them at 7625 Empire Drive, Florence, Kentucky 41042, call voice (800) 865-5840, facsimile (606) 647-5013, or send email to <[americas-info@list.thomson.com](mailto:americas-info@list.thomson.com)>

## **JANE'S INFORMATION GROUP**

Mr. Robert Loughman  
Sales Consultant  
1340 Braddock Place, Suite 300  
Alexandria, VA 22314  
Voice: (703)683-3700x202  
Fax: (703) 836-0297

The Jane's periodicals, database, and *SENTINEL* Country Series are "best in class" for military information. Jane's is also available online. It is important to know that Jane's only publishes 20% of what it knows, ask for unpublished info.

## **KROLL ASSOCIATES**

Mr. Thomas Fedorek, Managing Director  
900 Third Avenue  
New York, NY 10022  
Voice: (212) 593-1000  
Fax: (212) 593-2631

This is by all press and other accounts the world's best investigative firm, able to obtain scientific & technical information as well as other nominally sensitive information, using legal & ethical means.

## **LEXIS-NEXIS**

Mr. Jeff Krattenmaker  
Government Information Services  
9393 Springboro Pike, P.O. Box 933  
Dayton, OH 45401-0933  
Voice: (513) 865-1877  
Fax: (513) 865-7902

Together with DIALOG, one of the top two commercial online services, but perhaps best suited to be the "first stop", followed by DIALOG and other region-specific online services. "Government-friendly" and responsive.

## **Mercyhurst College**

Mr. Robert Heibel, Program Director, Research/Intelligence Analyst Program.  
Mercyhurst College, Department of History, Erie, Pennsylvania 16546. Voice: (814) 824-2117, fax: (814) 824-2219.

## **MONTEREY INSTITUTE OF INTERNATIONAL STUDIES**

Dr. Christopher Fitz  
Senior Manager  
PNS, 425 Van Buren Street  
Monterey, CA 93940  
Voice: (408) 647-4193  
Fax: (408) 647-3519

Uses graduate students fluent in Arabic, Russian, Vietnamese, and Korean, and other languages, to monitor media and maintain world's best unclassified database on proliferation--used by CIA's NPC.

## **NERAC**

Manager, New Business  
One Technology Drive  
Tolland, CT 06084-3900  
Voice: (203) 872-7000  
Fax: (203) 875-1749

Combines DIALOG and university experts to offer an annual "fixed price" research service that many businesses find to be responsive and cost-effective.

## ***netguide***

"TV Guide" of cyberspace  
Covers 60,000 bulletin boards  
9,000 networks. 500 libraries.  
all commercial online services  
384 pages. \$19.00. (800) 345-8112

As described--there are increasing numbers of such guides, most at higher prices. This is a good starting point.

## **NEWSEGE FROM DESKTOP DATA**

Ms. Emily Elliott, Assistant Marketing Manager  
Financial Markets  
1601 Trapelo Road  
Waltham, MA 02154  
Voice: (617) 672-2425  
Fax: (617) 890-1565

This unique service combines the normal current awareness service with the ability to deliver data directly into existing local area networks & database structures.

## **OXFORD ANALYTICA**

Mr. Robin Porteus  
Director of Client Services  
5 Alfred Street  
Oxford OX1 4EH  
UNITED KINGDOM  
Voice: (44 1865) 261-600  
Fax: (44 1865) 242-018

Founded by Mr. David Young, who served on the National Security Council with Dr. Henry Kissinger, this is the best international window into political and economic reporting. Combines the Dons of Oxford and 1000 experts worldwide, with a 24-hour media monitoring service.

### **PARVUS-JERICHO**

Mr. Gerard Burke, Chairman  
8403 Colesville Road  
Suite 610  
Silver Spring, MD 20910  
Voice: (301) 589-4949  
Fax: (301) 589-0007

After Kroll Associates, one of the best international investigative organizations. Mr. Burke served previously as the Executive Director of the President's Foreign Intelligence Advisory Board, and can support community needs.

### **Questel/Orbit**

Communicate with them at Questel/Orbit, Inc., France Telecom Group, 8000 Westpark Drive, McLean, VA 22102, voice (703) 442-0900, or facsimile (703) 898-4632.

### **RAPPORT RESEARCH & ANALYSIS (UK)**

Mr. Charles Pettifer, Director  
Mr. Kevin Dodd, Director  
11 Berkeley Street  
Mayfair, London W1X 6BU ENGLAND  
Voice: (44 171) 355-5020  
Fax: (44 171) 355-5021

This organization can provide trained debriefers fluent in any language to any place in the world. Especially good at canvassing refugee and emigre communities for raw intelligence.

### **RESEARCHBASE**

Mr. Frank J. Vega, President  
Post Office Box 187  
Arlington, VA 22210  
Voice: (703) 271-5988  
Fax: (703) 271-5989

This very low-cost (\$500) database is an essential means of saving money by avoiding redundant research in all major international relations areas. Tap into existing research for starters!

### ***Research Centers Directory***

Sometimes titled *Research Centers and Services Directory*. Available from Gale Research for \$400 (two volumes). ISBN 0-8103-7353X.

### **Rice University**

Call (313) 764-9366 to obtain information on gaining access to the Economic Bulletin Board Service (BBS).

### **RISA SACKS ASSOCIATES**

Ms. Risa Sacks, President  
3838 14th Avenue  
Oakland, CA 94602  
Voice: (510) 530-6154  
Fax: (510) 531-9086

Telephone surveys and telephone "discovery" of key elements of information is an art, and Ms. Risa Sacks is acknowledged by her peers as one of the best in the USA.

## **SCIENCE CITATION INDEX, SOCIAL SCIENCE CITATION INDEX**

### **Institute for Scientific Information**

Frank Spiecker  
3501 Market St.  
Philadelphia, PA 19104  
Voice: (215) 386-0100 ext.1374  
Fax: (215) 386-6362

This organization combines a citation database that will identify the latest articles based on known earlier publications, and also identify emerging technologies as well as key experts.

## ***Secrets of the Super Searchers***

By Reva Basch, 1993. Order directly from Eight Bit Books, 462 Danbury Road, Wilton, CT 06897-2126. ISBN 0-910965-12-9. \$39.95 plus shipping & handling.

## **SIS INTERNATIONAL RESEARCH**

Ms. Ruth Stanat, President  
490 South Main Street  
New City, NY 10956  
Voice: (914) 639-1934  
Fax: (914) 639-6936

Complements Fuld & Company with special strengths in Latin America and Asia; primarily a business/marketing research organization.

## **SPOT IMAGE CORPORATION**

Mr. Clark Nelson, Director of Communications  
1897 Preston White Drive  
Reston, VA 22091  
Voice: (703) 715-3100  
Fax: (703) 648-1813

They have, in hand, 10 meter resolution panchromatic and multispectral imagery for almost the entire world, and can produce both combat charts and simulations quickly.

## **STN International**

STN Service Center, c/o Chemical Abstracts Service, 2540 Olentangy River Road, Columbus, OH 43210. Voice: (800) 848-6533, facsimile (614) 447-3798. Email: <help@cas.org>.

## **The Reference Press, Inc.**

Among its offerings are a variety of directories and guides to international business sources and information for Latin America, Canada, Europe, Asia Pacific, and Russia. For a catalog call (512) 454-7778 or fax (512) 454-9401.

## **WORLDWIDE GOVERNMENT DIRECTORIES**

Mr. Jonathan Hixon, Publisher  
7979 Old Georgetown Road, #900  
Bethesda, MD 20814  
Voice: (301) 718-8770

Mr. Keith Hall invented the term "ASK-INT". This is the directory. They also publish government and military

Fax: (301) 718-8494

biographies for leaders worldwide.

#### **UNCOVER REVEAL**

Uncover Company  
3801 East Florida  
Suite 200  
Denver, CO 80210  
Voice: (303) 758-3030  
Email: <[mwhitaker@carl.org](mailto:mwhitaker@carl.org)>

Building on the University of Colorado's existing infrastructure, they will deliver for a nominal cost to your email or fax the tables of contents of all journals you wish, as they are published--then you can order articles from any source.

#### **UNITED PRESS INTERNATIONAL**

Ms. Alison Myers  
Director of Business Development  
UPI Photo Network  
Voice: (202) 898-8248  
Fax: (202) 371-8247

A picture can be worth a thousand words. Analysts interested in using visual images to improve the intelligence consumer's absorption of the intelligence product's content can call on this resource.

#### **University of Michigan**

Send electronic mail to <[lou@umich.edu](mailto:lou@umich.edu)> to obtain information on gaining access to the electronic clearinghouse.

## **APPENDIX E-1**

### **Internet: Self-Guided Tour**

by Dr. Ross Stapleton-Grey <director@embassy.org>

1. Philosophy
2. Strategies
3. Useful Tools
4. Starting Points
5. Print and Other Resources
6. USENET Illustration

#### **Philosophy**

The Internet is a steadily changing thing. What's there today will almost certainly be different tomorrow, either for the better, or for the worse! This poses a challenge when useful resources disappear, whether because they've been abandoned, or simply moved with no apparent forwarding address. On the other hand, hosts of new resources are being created every day... faster than they're being cataloged. The Internet has been described as "a wonderfully rich library, but all the books are lying in heaps on the floor."

The last few years have seen a number of wonderful navigational aids created, including powerful search engines, and comprehensive catalog sites for Web page creators to register their resources. But there will always be a place for serendipity, and certainly it helps to have a network of contacts and colleagues to pass along leads.

#### **Strategies**

The best strategy in looking for information via the Internet is to cast a broad net: Web sites will lead to others, or cite newsgroups or mailing lists, or vice versa, and human contacts made through the Internet can pass along useful nuggets.

All of the major Web browsers support "bookmarking," i.e., saving pointers to particularly useful or interesting destinations once you've found them (placing them on your "hotlist"). A helpful strategy is to bookmark all of the initial tools--query sites, or especially rich indexes--you might need, along with other sites you'll need to check regularly.

#### **Useful Tools**

The following are useful tools for the Internet (and especially, World Wide Web)



navigator. They can also be thought of as starting points: the skilled Internet navigator will make use of any number of search and catalog sites, to access familiar resources, or to launch off into undiscovered territory with a few search keywords.

Alta Vista - <http://altavista.digital.com>

One of the newest search engines, established by Digital Equipment Corporation (DEC), a major mid-range system manufacturer, as a technology demonstrator and a means to attract an audience. The service claims to index 8 billion words from some 16 million Web pages, and to continuously update its contents, retiring old materials no longer found, and adding new pages when encountered (some indexes don't--or can't--retire old pages, and may return links that lead to nowhere).

Alta Vista is the most impressive raw search engine for the World Wide Web thus far created. In addition to simple queries, one can structure complex searches, with weighted terms, and all of the usual Boolean search qualifiers. But the search tool has also been designed to meet the specific needs of Web navigators: one can search by date of the document (critical when what's needed is current information, and not some aging Web page with last year's news), and for URLs (Web page "universal resource locators," the "http:www.etc..."). The latter allows for neat tricks: check Alta Vista's help menus for directions on how to search for all of the Web pages that reference a certain other page, or how to find all of the pages mentioning certain terms, but which are not at some given address.

In addition to searching for Web pages, Alta Vista can search the most recent traffic in many of the USENET news groups.

Yahoo - <http://www.yahoo.com>

The most significant index in the Web's first major growth spurt, and the first comprehensive index of sites. Having one's Web site registered in Yahoo was (and is) a necessity. Yahoo involves human cataloging (submitters request where they would like to be filed, but Yahoo staff implement all linking), as opposed to the full-text indexers like Alta Vista. Where Alta Vista is an excellent tool to pull in anything and everything matching a given set of keywords, Yahoo's strength is in its organization. It would be extremely difficult to compile an exhaustive list of organizations in a given field by sifting through the mixed page of Web pages returned by Alta Vista; Yahoo will have a well-ordered index of companies divided and subdivided up according to a logical hierarchical structure. On the other hand, while Alta Vista vacuums up and indexes anything it can find on the Web, Yahoo is only as thorough as submitters and catalogers make it.

Yahoo also has an arrangement with Reuters to provide current newswire material through its site. The "Xtra" pages provide breaking items (a dozen or so per category) in Politics, News and World News, Business, Internet and Computers, and a half dozen other

areas.

<http://webcrawler.com>

An early full-text indexing tool, bought by America OnLine for more than a million dollars. It's included here largely for historical reasons, as other tools like Alta Vista seem to be eclipsing it. Webcrawler also has the annoying feature that it retains everything ever put in its index: pointers to Web pages that have been deleted long ago will still be found, and will give the user the famous "404 - URL Not Found" error when the link is followed.

A number of other services provide searching of extensive amounts of the World Wide Web, including OpenText (<http://www.opentext.com>) and Infoseek (<http://www.infoseek.com>).

### **Starting Points**

All of the search tools mentioned previously are excellent starting points. In addition to those, the following sites are rich indexes to their various areas:

NewsPage - <http://www.newspage.com>

NewsPage is a valuable site for industry information, including the telecommunications, energy, pharmaceutical and other industries. The site pools press releases and other news from a variety of other online services, and organizes them by category. While the site bases some of its revenues on advertising, it also charges premium subscription fees for some of its articles, and for use of a search facility.

Online Newspapers - various

Numerous "physical" news papers such as the Detroit News, San Francisco Chronicle, and New York Times have created Web versions to allow readers greater access to their stories, and to complement the print versions.

The Detroit News Web site (which was launched, coincidentally, as the print paper was in the middle of a union strike, and which has provided news on the strike as an editorial soapbox for the paper) is a good example of a Web site's use of a structured presentation: each day's format is identical, even if the content changes, providing a familiar layout. The Detroit News Website is at <http://detnews.com>.

Other good jumping off points to online newspapers:

Yahoo's newspaper index:

[http://www.yahoo.com/Business\\_and\\_Economy/Companies/Media/Newspapers/](http://www.yahoo.com/Business_and_Economy/Companies/Media/Newspapers/)

The Newspaper Association of America homepage : <http://www.intl.net/naa/hot.html>

The White House - <http://www.whitehouse.gov>

In addition to holding information on the White House, the Executive Office of the President, and the texts of presidential and vice presidential speeches, the White House Web site is the "site of sites" for the Federal Executive Branch. White House staff have taken considerable care to encourage Federal agencies to provide Web addresses, and the site indexes all of the major cabinet offices and a great many of the other agencies, bureaus and programs.

The WELL's War Conference, IW sites -  
<http://www.well.com/conf/war/iwsites.html>

Participants in the War conference on the WELL (a large online conferencing system based in Northern California but with users worldwide) have compiled an extensive reference of Web sites of interest to the "Information Warrior" (largely of defense, economic security and intelligence related sites). Some of the sites included on the list (a small sampling):

The White House's Information Infrastructure Task Force - <http://www.iitf.doc.gov>

Office of the Secretary of Defense - <http://enterprise.osd.mil>

US Air Force - <http://www.afin.af.mil>

Air Force 38th E&I Wing - <http://www.eiw38.af.mil/cshome.html>

Central Intelligence Agency - <http://www.odci.gov/cia>

Intelligence Community - <http://www.odci.gov/ic>

Electronic Embassy - <http://www.embassy.org>

The Electronic Embassy Web site is an index to information, including Web homepages where available, from the foreign embassy community in Washington D.C.

All of the above ought to be considered merely starting points, and most lead quickly to many other resources. The White House site is an exhaustive list of Federal agencies, while the Electronic Embassy is a quick shortcut to find the State Department, foreign affairs committees of the Congress, or the United Nations.

The more the Internet begins to parallel the "real world," that is, as having a Web site becomes the rule for companies, and not just the innovative exception, traditional clearinghouses will have a role to play. The Software Publishers Association (<http://www.spa.org>), for example, has long been an advocacy organization for the software industry, with a large number of the most significant software producers as members. The SPA Web site, extending its member services onto the Internet, provides a lengthy index to all of its members, with pointers to their own Web sites.

There are excellent "theme" pages created by individuals, compiling exhaustive lists of known resources on the Web under a given topic area. These might range from Feminist Activist resources (Sarah Stapleton-Gray's page at IGC - <http://www.igc.org/women/feminist.html>) to anything and everything related to telecommunications organizations, technologies and policy (Jeff MacKie-Mason's page at the University of Michigan, <http://www.spp.umich.edu/telecom-info.html>). While one could try to compile a list of these lists (and to some extent such a thing has been done with Yahoo), spending even a small amount of time "surfing" the Web is guaranteed to turn up such useful references, which can then be bookmarked.

## **Print and Other Resources**

The nature of the Internet is such that virtually any print resource, and certainly any that attempts to document an exhaustive list of anything, be it USENET newsgroups or "the best Web sites for...", becomes obsolete in a manner of months. That said, there are some fairly useful books on various aspects of the Internet and the World Wide Web, which can give a good feel for the tools and the Internet's content, while recognizing that any given list of Web sites will have changed even as the book went to the printers.

The O'Reilly and Associates series of books are essential reading for the nuts and bolts of how the Internet works. *The Whole Internet User's Guide and Catalog* is a basic primer, with extensive (but, of course, fast-aging) lists of useful sites, mailing lists and newsgroups. *Managing Internet Services* provides extensive information on the technical details of Gopher, Majordomo (mailing list software) and the World Wide Web--not for the novice but providing for a complete understanding of how all of these features actually work.

*HTML Sourcebook*, by Ian S. Graham (John Wiley & Sons, publisher) is a good overview of how to create pages for the World Wide Web, again providing good insight into how the Internet supports the Web, and how Web sites work. The book provides walk-throughs of several actual sites, dissecting them to show how the Web can be used to deliver information, query users using forms, etc.

Members of the Internet Society receive its "On The Internet," a bi-monthly magazine on Internet issues and features. Individual membership in the Society is \$35 per year. ISOC may be reached at:

The Internet Society  
12020 Sunrise Valley Drive, Suite 210  
Reston VA 22091  
(703) 648-9888

ISOC also has a Web site:  
<http://www.isoc.org> as does its  
DC area chapter:  
<http://www.dcisoc.org>

## USENET Illustration

NOTE: For each of these, the first column is the message number. the second column shows the number of replies, if any, followed by the message title and the poster's userid.

From soc.culture.kuwait:

97	+	(FWD) BAHRAIN: Amnesty Int'l Appeal	socakh@pmail ldc.lu.se
98	+	TEST -- ignore -- TEST --	Furqan (truth@reality.com
99	+	2 (Fwd) Bahrain News/more	socakh@pmail ldc.lu.se
100	+	Test!! Please ignore	Badran (badran@kuwait.net
101	+	Online Zakat Payment	Sohail Mohammed (zakat@di
102	+	3 My visit to Kuwait	Lee Cooper (leec@kuwait.n
103	+	2 WANTED: STAMPS.....PLEASE,.....PLEA	Carol (carol@cam.org)
104	+	2 Immigrate To C A N A D A	lfrank@interlink.net
105	+	WWW Islamic Server: What's New!	Muslim Student Associatio
106	+	Canada - employment opportunities	Colin R. Singer (csinger@
107	+	-How can we benefit from the Internet?	Al-Sirat Al-Mustaqeem Mag
108	+	3 "I love you" in many languages Re: Ple	Gaspar Rodriguez (grodrig
109	+	Telethon for Islamic Centre for Kingst	Thomas (Aalim Zakee) Feve
110	+	3 SMITH	Sbostic@lovetts.com
111	+	Ramadhan Radio 107.4 FM. London	m.asghar@ic.ac.uk
112	+	2 arranged marriages	Shoba Narayan (shoba@i-20

From alt.current-events.bosnia:

113	+	"Vise-parlamentarizam" -- metod veleiz	Y Rapido (rapido@eskimo.c
114	+	3 Wars for Succesion of Yugoslavia / WEB	d.d. chukurov (ddc@bellco
115	+	Yugoslav Daily Survey. 2/2	d.d. chukurov (ddc@bellco
116	+	Serbia Today, 2/2	d.d. chukurov (ddc@bellco
117	+	Yugo Wars - Stay Informed - Visit : g	d.d. chukurov (ddc@bellco
118	+	2 Michael Axelrod strikes again	Frank Hendrix (Frank@accl
119	+	7 Army witch hunts	RICHARD CASTROP (RCASTROP
120	+	Yugo Wars - Stay Informed - Visit : Vu	Barry S. Marjanovich (bsm
121	+	3 appeal	barala@vossnet.co.uk
122	+	The three religius groups Moslem, east	Ben (smillieb@the.link.ca
123	+	Novi "bogovi" - "Hrvatska domovna" 12/	BorPet (borpet@aol.com)
124	+	idea: low-tech approach to safely remo	JGizdavic (jgizdavic@aol.
125	+	Bosnain to English dictionary	JGizdavic (jgizdavic@aol.
126	+	Serbia Today (After SREBRENICA)	Barry S. Marjanovich (bsm
127	+	Britain, Rose, SAS Stab-in-the-Back--t	Y Rapido (rapido@eskimo.c
128	+	YUGOSLAV WEEKLY SURVEY, 2/2	D.D. Chukurov (ddc@nyquis

From alt.politics.org.un:

97 + 6 WAR ON THE FED waged by Utah's Patriot Tony Kimball (alk@pobox.c  
98 + UN Daily Highlights: 29 Jan, 1996 (Rev Shawn H (c626193@mizzoul.  
99 + United Nations Update: 30 Jan, 1996 Shawn H (c626193@mizzoul.  
100 + 6 Steve Forbes as a Phony Candidate root (root@tailor.roman.o  
101 + United Nations Association of the Unit Shawn H (c626193@mizzoul.  
102 + 6 GORE CLINTON OUT Fresh816 (fresh816@aol.co  
103 + United Nations Update: 31 Jan, 1996 Shawn H (c626193@mizzoul.  
104 + 2 U.S. Public Support for U.N. Growing ( Rodney L. Cornelius (CORN  
105 + 3 Slick Willie as a Phony Candidate Mark O. Wilson (Mark.O.WI  
106 + U.S. Must Pay U.N. Dues says Defense W Al Banner (ac590@FreeNet.  
107 + ----Gen X Presidential Forum!!! Mike Lee (mlee@harvard.ed  
108 + 3 New site: Electronic Field Trip to th Nancy K (nancyk@bga.com)  
109 + 2 Setting the Record Straight (The UN I Nancy K (nancyk@bga.com)  
110 + What is next for Michael New? Archibald E. Roberts, LtC  
111 + United Nations Update: 1 Feb. 1996 Shawn H (c626193@mizzoul.  
112 + 3 Michael New Boulder Weekly (bweditor@

## APPENDIX E-2

### Intelligence-Oriented List of Useful Internet Sites

From the Staff of OSS, Inc. <oss@oss.net>

NOTE: The material which follows focuses primarily on World-Wide Web (www) sites because that is the overwhelmingly most productive environment. Gopher sites (menus providing access to text) and File Transfer Protocol (FTP) sites are still available but declining so quickly as to hardly be worth citing. Also, it is important to do your own searches for sites and to regularly update your lists. The Net is growing geometrically, and sites emerge (or die) every day. The sites listed below are simply illustrative, and by no means comprehensive. Besides regular searches of the www, analysts should subscribe to ListSerts in their areas of interest--these deliver documents directly to an email address, and also allow for analysts to contribute commentary to the list for rebroadcast to others.

#### Top Guns

<http://www.oss.net/oss/>

The home page of OPEN SOURCE SOLUTIONS, Inc., a non-profit educational corporation that serves as an international clearinghouse for information about open sources, systems, and services, this site provides past issues of *OSS NOTICES* for free, and is soon to offer, also for free, digital copies of the two volume *Proceedings* from each of the annual conferences on open sources which have taken place since 1992. This site offers direct links to a number of other open source vendors and pertinent sites for open source intelligence.

<http://www.tiac.net/users/jardines/434mid.html>

These heavy-duty reservists, the 434th Military Intelligence Detachment (Strategic), created the first-ever *Open Source Intelligence Resources for the Military Intelligence Officer*, and kicked off an Army-wide effort that is now leading joint concepts and doctrine on the integration of open source intelligence into the all-source collection and production process.

<http://www.awpi.com:80/IntelWeb/>

The home page of *Intelligence Watch Report*, a daily electronic clipping service for intelligence-related news, and the only service of its kind focused strictly on national intelligence. Benefits from correspondents in Europe, Russia, and Asia.

<http://www.fedworld.gov/>

FedWorld, the central point of access to the entire U.S. government, very ably

developed and maintained by the National Technical Information Service, a self-sustaining activity of the Department of Commerce.

## United States Government

<http://www.whitehouse.gov/>  
<http://www.loc.gov/>  
<http://thomas.loc.gov/>

The White House  
The Library of Congress  
U.S. Legislation OnLine.

**United States Intelligence**

<http://www.odci.gov>  
<http://www.nsa.gov:8080/>  
<http://www.fbi.gov/>  
<http://www.ustreas.gov/treasury/bureaus/usss/usss.html>  
<http://www.fas.org/pub/gen/fas/irp/nro/index.html>  
<http://www.awpi.com/IntelWeb/US/NCC/index.html>

Central Intelligence Agency  
National Security Agency  
Federal Bureau of Investigation  
U.S. Secret Service  
National Reconnaissance Office  
National Counterintelligence Center

**United States Military**

http://www.dtic.mil/defense/defenselink/osd/index.html  
http://www.dtic.mil/defense/defenselink/osd/index.html  
http://www.army.mil/  
http://www.dot.gov/dotinfo/uscg/  
http://www.dtic.mil/airforcelink/  
http://www.dtic.mil/airforcelink/  
http://www.navy.mil/navresfor/  
http://www.hqmc.usmc.mil/  
http://www.dot.gov/dotinfo/uscg/  
http://www.dtic.dla.mil/c3i/  
http://www.dtic.dla.mil/dtiw/

OSD  
Joint Chiefs of Staff  
U.S. Army  
U.S. Army Reserve  
U.S. Air Force  
U.S. Navy  
U.S. Naval Reserve  
U.S. Marine Corps  
U.S. Coast Guard  
OSD C3I  
Defense Technical  
Information Center

<http://www.onestep.com:80/milnet/>  
MILNET: Open Source Military Information Database

<http://www.dtic.dla.mil/defense/defenselink/pubs/pentagon/index.html>  
The Pentagon  
<gopher://marvel.loc.gov/70/11/federal/fedinfo/byagency/military/>  
US DOD Gopher Sites

[http://www.dtic.mil/airforcelink/pa/factsheets/Air\\_Force\\_Reserve.html](http://www.dtic.mil/airforcelink/pa/factsheets/Air_Force_Reserve.html)  
USAF Reserve



<http://pages.prodigy.com/AL/20sfga/mid20sfga.html>  
Military Intelligence: 20th Special Forces Group

## **United States Unified Commands**

<a href="http://www.dtic.mil/defense/defenselink/factfile/chapter1/eucom.html">http://www.dtic.mil/defense/defenselink/factfile/chapter1/eucom.html</a>	U.S. European Command
<a href="http://www.dtic.mil/defense/defenselink/factfile/chapter1/pacom.html">http://www.dtic.mil/defense/defenselink/factfile/chapter1/pacom.html</a>	U.S. Pacific Command
<a href="http://www.dtic.mil/defense/defenselink/factfile/chapter1/pacom.html">http://www.dtic.mil/defense/defenselink/factfile/chapter1/pacom.html</a>	U.S. Atlantic Command
<a href="http://www.dtic.mil/defense/defenselink/factfile/chapter1/southcom.html">http://www.dtic.mil/defense/defenselink/factfile/chapter1/southcom.html</a>	U.S. Southern Command
<a href="http://www.dtic.mil/defense/defenselink/factfile/chapter1/centcom.html">http://www.dtic.mil/defense/defenselink/factfile/chapter1/centcom.html</a>	U.S. Central Command
<a href="http://www.dtic.mil/defense/defenselink/factfile/chapter1/spacecom.html">http://www.dtic.mil/defense/defenselink/factfile/chapter1/spacecom.html</a>	U.S. Space Command
<a href="http://www.dtic.mil/defense/defenselink/factfile/chapter1/socom.html">http://www.dtic.mil/defense/defenselink/factfile/chapter1/socom.html</a>	U.S. SpecOps Command
<a href="http://infosphere.safb.af.mil/TRANSCOM/">http://infosphere.safb.af.mil/TRANSCOM/</a>	U.S. TransCom
<a href="http://www.dtic.mil/defense/defenselink/factfile/chapter1/stratcom.html">http://www.dtic.mil/defense/defenselink/factfile/chapter1/stratcom.html</a>	U.S. StratCom

## **Related U.S. Sites**

<a href="http://huachuca-usaic.army.mil/">http://huachuca-usaic.army.mil/</a>	USAIC/Schoolhouse
<a href="http://www.dtic.dla.mil/dtiw/">http://www.dtic.dla.mil/dtiw/</a>	Defense Technical Information Web

<gopher://UMSLVMA.UMSL.EDU:70/11/LIBRARY/GOVDOCS//BNOTES>  
U.S. State Department Country Reports

<http://www.esd.ornl.gov/doe-labs/doe-labs.html>  
(U.S. Department of Energy National Laboratories & Programs)

<http://dosfan.lib.uic.edu/>  
(Department of State Foreign Affairs Network)

## **Associations & Organizations**

<a href="http://www.cais.com/NMIA/HomePage.html">http://www.cais.com/NMIA/HomePage.html</a>	National Military Intelligence Association
<a href="http://www.cais.com/zhi/OPSHomePage.html">http://www.cais.com/zhi/OPSHomePage.html</a>	Operations Security Professionals Society
<a href="http://www.loyola.edu/politics/intel.html">http://www.loyola.edu/politics/intel.html</a>	Loyola Page on Strategic Intelligence
<a href="http://www.acsp.uic.edu/oicj/pubs/">http://www.acsp.uic.edu/oicj/pubs/</a>	Office of International Criminal Justice
<a href="http://www.cdi.org/">http://www.cdi.org/</a>	Center for Defense Information
<a href="http://nsi.org/">http://nsi.org/</a>	National Security Institute
<a href="http://www.eff.org/govt.html">http://www.eff.org/govt.html</a>	Electronic Frontier Foundation

## **More Related Publications**

<a href="http://www.jeddefense.com/jed.html">http://www.jeddefense.com/jed.html</a>	Journal of Electronic Defense
---	-------------------------------

<http://ursula.blythe.org/NameBase>

NameBase News

<http://www.worldmedia.com/caq/>

Covert Action - Home Page

<http://www.awpi.com/IntelWeb/US/S-GB/index.html>

Secrecy & Government Bulletin

## Cyber War

<http://www.tcst.com/~tighe/>

Mike Tighe's Cryptology Home Page

<http://www.psychom.net/iwar.1.html>

Information Warfare, I-War, Cyberwar

<http://www.disa.mil/ciss/itso.html>

DISA - Information Security

<http://all.net/>

InfoSec

<http://freeside.com/phrack.html>

Phrack - underground hacker magazine

<http://www.gocsi.com/>

Computer Security Institute

<http://dubhe.cc.nps.navy.mil/~budden/>

IW - US Navy

<http://www.cse.dnd.ca/~formis/>

IW - Resources

[http://www.csto.arpa.mil/ResearchAreas/Defensive\\_Information\\_Warfare.html](http://www.csto.arpa.mil/ResearchAreas/Defensive_Information_Warfare.html)

IW database

<http://carmen.artsci.washington.edu/propaganda/contents.htm>

Propaganda - Disinformation Warfare

<http://www.monmouth.army.mil/peoiew/peoiew.html>

Intelligence and Electronic Warfare

## Foreign Countries - US Sources

<gopher://UMSLVMA.UMSL.EDU/11/LIBRARY/GOVDOCS/ARMYAHBS>

US Army - Foreign Intelligence Agencies

<gopher://UMSLVMA.UMSL.EDU:70/11/LIBRARY/GOVDOCS//BNOTES>

US State Dept.: Report by Country

<gopher://UMSLVMA.UMSL.EDU:70/11/LIBRARY/GOVDOCS//WF93/WFLATEST>

US CIA: Report by Country

<http://www.ncsa.uiuc.edu/SDG/Experimental/soviet.exhibit/soviet.archive.html>

Library of Congress Soviet Archives Exhibit

## Foreign Countries

<http://watserv1.uwaterloo.ca/~brobinso/cse.html>

The Unofficial Communications Security Establishment Webpage

<http://www.reading.ac.uk:80/SecInt/>  
Great Britain - SECURITY AND INTELLIGENCE

<http://www.awpi.com/IntelWeb/Palestine/index.html>  
Palestinian Intelligence Community

<http://www.primenet.com/~lion/j.html#issue>  
USSR - The Third World Countries & US

<gopher://infx.infor.com:4600/11.browse/ESPIONAGE>  
ESPIONAGE - publications

<http://www.odci.gov/mapspub/index.html>  
CIA Maps & Publications

### **On-line Search**

<a href="http://webcom.com/%7Epinknoiz/covert/ciabasesearch.html">http://webcom.com/%7Epinknoiz/covert/ciabasesearch.html</a>	CIABASE On-line
<a href="http://www.btg.com/janes/">http://www.btg.com/janes/</a>	BTG Jane's EIS - on-line
<a href="http://www.janes.com/janes.html">http://www.janes.com/janes.html</a>	Jane's Information
<a href="http://www.mayhem.net/Crime/">http://www.mayhem.net/Crime/</a>	Crime Archives
<a href="ftp://wiretap.spies.com/">ftp://wiretap.spies.com/</a>	Directory of Wiretaps
<a href="ftp://ftp.lglobal.com/pub/foreignc/">ftp://ftp.lglobal.com/pub/foreignc/</a>	The Foreign Correspondent:

<http://world.std.com/~mmoore>  
INVESTIGATIVE DATABASE: Boston, MA

<http://www.delve.com/consort.html>  
The Consortium - Investigative Reports

<telnet://ursula.blythe.org>  
NAMEBASE telnet version - telnet gateway required. Log in as "namebase"

<http://ursula.blythe.org/NameBase/bookindx.html>  
NAMEBASE - Web version

### **Military Intelligence - Non-Governmental Resources**

<http://www.infomanage.com/international/intelligence/default.html>  
Intelligence Resources

<http://www.cdi.org/>  
Center for Defense Information

<http://www.tscm.com/>  
TSCM.COM Counterintelligence Home Page

<http://www.interlog.com/~vahirol/>  
Counter-Terrorism

<http://www.interport.net/~sagal/ajax.html>  
AJAX MILITARY, INTELLIGENCE & LAW ENFORCEMENT AGENCY ACCESS

<http://www.acsp.uic.edu/oicj/pubs/>  
Office of The International Criminal Justice

<http://www.essential.org/nautilus/>  
Nautilus Institute for Security and Sustainable Development

<http://www.fas.org/pub/gen/fas/>  
Federation of American Scientists Home Page </A> <br>

<http://www.usdoj.gov/ojp/rol/docs/home.html>  
Rule of Law Online

<http://www.webcom.com/%7epinknoiz/politics.html>  
Political Investigations

<http://www.interaccess.com/trc/tsa.html>  
Technical Services Agency

<http://www.rssi.ru/>  
Russian Space Science

<http://www.peak.org/~danneng/decision/int-law.html>  
War Crime Laws

### **United States Military & Defense Laboratory Servers**

<http://www.arc.umn.edu/html/ahpcrc.htm>  
Army High Performance Computing Research Center

<http://www.arpa.mil/>  
Advanced Research Projects Agency

<http://bradbury.nrl.navy.mil/general/bmdo.html>  
Ballistic Missile Defense Organization Test Data Centers

<http://www.dtic.dla.mil:80/lablink/>  
(U.S. Department of Defense Laboratory System)

<http://www.nrl.navy.mil/>  
The Naval Research Laboratory

<http://www.rl.af.mil:8001/>  
(USAF Rome Laboratory for C4I Technology)

### **Weapons and Their Transfers**

<Gopher://csf.colorado.edu:7011/peace/pubs>  
General information

<http://www.atcon.com/stores/armament/index.htm>  
Armament Technology

<http://www.pal.xgw.fi/hew/>  
The High Energy Weapons Archive

<http://nuke.handheld.com/>  
Nuke Home Page

<http://neutrino.nuc.berkeley.edu/neutronics/todd.html>  
Todd's Atomic Homepage

<http://www.earthlink.net/~bkonop/GermIncidents2.html>  
GERM WARFARE

<http://www.opcw.nl/guide.htm>  
The Chemical Weapons Convention

<http://www.aber.ac.uk/~ctj94/>  
Bombs 'n' Bullets

<http://www.umcc.umich.edu/~schnars/texte/fore-cod.htm>  
Code Names and Numbers for Weapons

### **Law Enforcement**

<http://www.ustreas.gov/treasury/bureaus/atf/atf.html>  
Bureau of Alcohol, Tobacco and Firearms

<http://gopher.usdoj.gov/bureaus/bop.html>

## **Federal Bureau of Prisons**

<http://www.ustreas.gov/treasury/bureaus/fincen/fincen.html>  
Financial Crimes Enforcement Network

<http://www.ustreas.gov/treasury/bureaus/fletc/fletc.html>  
Federal Law Enforcement Training Center

<http://gopher.usdoj.gov/bureaus/usm.html>  
U.S. Marshals Service

<http://nletc.aspensys.com:83/nletchome.html>  
National Law Enforcement Technology Center

<http://www.ustreas.gov/treasury/bureaus/usss/usss.html>  
Secret Service

<http://www.gate.net/~customs/>  
U.S. Customs Service Office of Investigation

## **Commercial Intelligence & Industrial Espionage**

<http://w3.lanter.net/NEWR/>  
<http://infomanage.com/icr>  
<http://www.webcom.com/~thames/spy/>  
<http://www.jax-inter.net/ispy/>  
<http://www.ipn.net/>

NEAL E. WILSON RESEARCH  
Asia Business Intelligence  
MIND YOUR OWN BUSINESS  
Somers & Associates  
Information Professionals Network

## **Security Resources & Services**

<http://nsi.org/>  
<http://www.ozemail.com.au/~hotsec/index.html>  
[http://www.fsk.ethz.ch/D-REOK/fsk/defs\\_intn.html](http://www.fsk.ethz.ch/D-REOK/fsk/defs_intn.html)  
<http://www.t8000.com/eci/brief.htm>  
<http://chelsea.ios.com/~glenz/>  
<http://www.canadamalls.com/provider/horvath.html>  
<http://www.w2.com/docs2/z/spyshop.html>  
<http://www.hometeam.com/apex.shtml>  
<http://www.trcone.com/tsa.html>  
<http://www.ozemail.com.au/~hotsec/hitec.htm>  
<http://www.iapps.org/>  
<http://www.best.com/~cntrspy/>  
<http://www.shadow.net/~trinfol>  
<http://www.wta.com/giin/>

Security Resource Net  
HTSCORP Home Page  
International Security Network  
Cellular Surveillance Systems  
Corporate Security - Sigma Group  
The Spy Depot  
THE SPY SHOP  
Apex Home Page  
The Codex Home Page  
HI TECH Securities Services  
Bodyguard Home Page  
Bodyguard  
TR Information Services  
Global Investigations & Information

<http://www.tiac.net/users/cgb/din>  
<http://www.mja.net/pub/continen/>  
<http://www.integctr.com/>  
<http://lainet3.lainet.com/factfind/>  
<http://www.tecs.com/irrs>

Detective Information Network  
Continental Investigative Service  
Integrity Center: Risk Management  
Investigative Resources  
Investigators Resource and Referral

[http://www.yahoo.com/Business/Products\\_and\\_Services/Security/](http://www.yahoo.com/Business/Products_and_Services/Security/)  
Yahoo - Security </A> <br>

[http://www.yahoo.com/Business/Corporations/Investigative\\_Services/](http://www.yahoo.com/Business/Corporations/Investigative_Services/)  
Yahoo - Investigative Services

### **International**

<http://www.ifs.univie.ac.at/~pr2gq1/uno>  
United Nations Crime Prevention & Criminal Justice

<http://daedalus.dra.hmg.gb/>  
Defence Research Agency, United Kingdom

<http://www.dreo.dnd.ca/>  
Defense Research Establishment, Ottawa, Canada

<http://www.nato.int>  
North Atlantic Treaty Organization

### **Usenet Groups**

<news:alt.politics.org.cia>  
<news:alt.politics.org.fbi>  
<news:alt.politics.org.nsa>  
<news:alt.conspiracy.amer51>  
<news:sci.crypt>  
<news:talk.politics.crypto>

## APPENDIX E-3

### Intelligence (Related) Sites from *PC Magazine's* Top 100 Web Sites

Selected by the Staff of OSS, Inc. <oss@oss.net>

NOTE: The sites listed below are drawn from "Web Sites 100: PC Labs Rates the Top 100", in *PC Magazine* Volume 15, Number 3 (6 February 1996). The quickest way to explore all of these sites is through the online version of the story, available at <<http://www.pcmag.com>>, where the list will also be constantly updated.

#### Computer Resources

BrowserWatch <http://www.ski.mskcc.org/browserwatch/>

The best place to follow emerging Internet browser tools.

O'Reilly and Associates <http://www.ora.com>

Publishers of such respected books as *Computer Crime: A CrimeFighter's Handbook*, this organization is a good place to identify educational materials for all aspects of Internet research.

#### News & Sports

CNN Interactive <http://www.cnn.com>

Includes a video vault as well as a keyword search tool for past CNN stories. Could be the ideal source for downloading film and sound "snapshots" for a multi-media briefing.

*Electronic Telegraph* <http://www.telegraph.co.uk/>

The respected London newspaper.

Reuters NewMedia <http://www.yahoo.com/headlines/current/news>

Rapid bare-bones reporting, strictly text-based.

*Time Magazine* <http://www.pathfinder.com/time>

Everything you would expect, including *Time Daily*, late-breaking news.

*USA Today* <http://www.usatoday.com>



Retains its graphical excellence. Includes cyber-listings.

## **Government & Politics**

FedWorld Information Network     <http://www.fedworld.gov/>

Access to over 130 government bulletin boards as well as many government Web and gopher sites.

GPO Gate     <http://ssdc.ucsd.edu/gpo>

Includes full-text of major GPO publications such as the *Federal Register*, *Congressional Record*, Senate and House calendars, and the United States Code.

The Library of Congress     <http://www.loc.gov>

Includes THOMAS, a Web version of the *Congressional Record*, and other Capitol Hill publications. Often mis-represented as providing access to 70 million actual documents, what it really provides is access to the listing of such documents. It does have some full text material.

The United Nations     <http://www.un.org>

Marginal in terms of substance, but some conference updates, news releases, and Security Council information.

## **Reference**

Britannica On-Line     <http://www.eb.com>

Costs money (\$25 registration, \$150 per year). Includes same content as bound edition, articles not yet in print, *Britannica Book of the Year*, and *Webster's Dictionary*.

CityNet     <http://www.city.net>

While not a comprehensive guide, it does cover sites from Scotland to Africa, and is an interesting illustration of the kind of beach surveys and city maps that might one day be available to arriving military forces accessing the Internet from their landing platforms.

Science, Technology, & Medicine     [http://www.asap.unimelb.edu.au/hstm/hstm\\_ove.htm](http://www.asap.unimelb.edu.au/hstm/hstm_ove.htm)

Historical in nature, part of the Virtual Library, includes biographical information,

documents on every area of technology, a directory of scientific institutions, and electronic journals.

## APPENDIX E-4

### HOW TO FIND AN INTERESTING MAILINGLIST

Arno Wouters - Arno.Wouters@phil.ruu.nl  
(with minor modifications by OSS, Inc. staff)

Last update: 5 February 1994

This document is available by email from "listserv@vm1.nodak.edu" with "GET NEW-LIST WOUTERS" or by anonymous ftp from "vm1.nodak.edu" as "new-list.wouters" in the directory "new-list".

(In compiling this information I have made ample use of Marty Hoag's "Some lists of list" (as of 05/01/92) which is retrievable from NEW- LIST as "LISTSOF LISTS")

#### TABLE OF CONTENTS

GENERAL INFORMATION ABOUT MAILINGLISTS

TWO NOTES ON ADDRESSES

SOURCES

TOOLS and METHODS

The LISTSERV "List of lists"

The SRI NISC "interest-groups" list of lists

The USENET lists of newsgroups and mailing lists

The Dartmouth SIGLIST

The "Directory of Scholarly Electronic Conferences" (ACADLIST)

NEW-LIST

LIST SEARCHES ON THE INTERNET

#### GENERAL INFORMATION ABOUT MAILINGLISTS

A mailing list is a computer program that distributes messages among a list of subscribers. This program has an email-address (listname@domain). Mail sent to this address is distributed automatically to all the subscribers.

There are two types of mailing lists: manually maintained lists and automated lists.

(1) In its manual form the list of subscribers is maintained by a person, the list administrator. To subscribe to such a list one should ask the list administrator to add you to the list. Typically the administrator can be reached at listname-request@domain.

(2) An automated list is maintained by a program (a so-called mailserver). To (un)subscribe to an automated list one should send a message to the mailserver. Usually,

this is the command "SUB listname Yourfirstname Yourlastname" to subscribe and "SIGNOFF listname" to sign off (substitute the appropriate names and leave off the quotes!).

A mailserver is a program that interprets the lines in a message as a series of commands to act on, for example to mail a file or to add a person to a mailing list. To learn how to handle a mailserver one should send a one line message containing the command "help" (no quotes!) to the mailserver's address. (In some rare cases, the mailserver needs an empty message with "help" in the subject).

LISTSERV is the name of the single most important mailserver on Bitnet. It provides three kinds of services: (1) mailing list management, (2) file archives, and (3) address registration. A userguide is available from [LISTSERV@EARNCC.BITNET](mailto:LISTSERV@EARNCC.BITNET) by sending it the command GET LSVGUIDE MEMO. The command HELP can be sent to any Listserv. It will give you a short list of commands. "INFO REFCARD" returns a longer list, "INFO GEN" a manual. Typically, if a list's address is [LIST@NODE.BITNET](mailto:LIST@NODE.BITNET) the list is maintained by [LISTSERV@NODE.BITNET](mailto:LISTSERV@NODE.BITNET). Alternatively, if [LISTSERV@NODE.BITNET](mailto:LISTSERV@NODE.BITNET) maintains a list named LIST the list's address is [LIST@NODE.BITNET](mailto:LIST@NODE.BITNET).

There are also Unix versions of Listserv that work on the Internet. Don't expect these versions to function exactly like the traditional Listserv.

**IMPORTANT:** One should carefully distinguish between the address of the list and the address of the administrator/mailserver. Never send requests/commands for (un)subscription to the list! Such a message would bother all the participants, but it would not help you to get on/off the list. Note, that the list administrator is often just that: one of the computer people who maintains the list, but is not himself a subscriber. Alternatively, a mailserver will only react to mail that is addressed to the mailserver's address, not to the address of the lists it maintains.

<u>Type of list</u>	<u>Address of list</u>	<u>Requests/commands</u>
Manually	<a href="mailto:listname@domain">listname@domain</a>	<a href="mailto:listname-request@domain">listname-request@domain</a>
LISTSERVed	<a href="mailto:listname@node.BITNET">listname@node.BITNET</a>	<a href="mailto:LISTSERV@node.BITNET">LISTSERV@node.BITNET</a>

### TWO NOTES ON ADDRESSES

Internet addresses have the format [user@domain](mailto:user@domain) (for example [John.Doe@phil.ruu.nl](mailto:John.Doe@phil.ruu.nl)). Bitnet uses the format [user@bitnetnode](mailto:user@bitnetnode) (for example [JDOE@HNYKUN51](mailto:JDOE@HNYKUN51)). To send mail from Internet to Bitnet append ".BITNET" to the Bitnet address (e.g. [JDOE@HNYKUN51.BITNET](mailto:JDOE@HNYKUN51.BITNET)). To send mail from BITNET to Internet one could use the Internet address without any changes.

Janet users in the United Kingdom should reverse the order of the Internet domainnames and Internet users outside the UK should reverse the order of Janet domainnames.

There are several lists of lists available. The main ones are:

- the Listserv "list of lists" on Bitnet;
- the Internet "interest-groups" list;
- two lists of Usenet newsgroups:
- the Usenet list of "Publicly Accessible Mailing Lists" on Internet and UUCP networks;
- a combined list of Bitnet and Internet lists from Dartmouth (SIGLIST);
- the "Directory of Scholarly Electronic Conferences" (ACADLIST), an annotated list of mailing lists, newsgroups, newsletters, electronic journals etc. that are of interest to academics;

Another important sources is:

- NEW-LIST, a Listserved mailing list and archive for announcements of new lists. In addition, the NEW-LIST archive contains copies of both the Listserv and the "interest-groups" lists of lists in a searchable format.

NOTE: The WAIS based "lists" database on CIC-net has been dissolved.

## TOOLS and METHODS

Basically, there are two methods to access these sources:

- (1) on line searches
- (2) retrieve a list and search through it at home (electronically or after printing).

As most lists are long, the first method is often the preferred one.

Internet tools for on line retrieval: gopher, WAIS, telnet (one tool would suffice, gopher is the preferred one for lists).

Listserv databases can be searched interactively from VAX/VMS and from VM/SP CMS systems. Other users should submit batch jobs by email. Send an "INFO DATABASE" to an appropriate Listserv for more information.

Tools for retrieving files: anonymous ftp (Internet only) and email. Make sure you have enough disk space available, since most lists are VERY long.

Tools for searching the retrieved files include your favorite word processor, GREP commands, hypercard etc.

#### The LISTSERV "List of lists"

The Listserv list of lists contains one line descriptions of Listserved lists on Bitnet. Most (but not all) Listservs will get you a copy after submitting the command "LIST GLOBAL". Most servers would also allow for the command "LIST GLOBAL /string" (e.g. "LIST GLOBAL /philos") to get those lists which have "string" in their description.

#### The SRI NISC "interest-groups" list of lists

This is a list with descriptions of special interest group mailing lists available on the Internet, compiled by Steven Bjork. New versions of this list are typically issued on a quarterly basis.

The file "interest-groups" (over 1.2 MB!) is available: by anonymous ftp from sri.com in the directory "netinfo", or by email from mail-server@sri.com ("send interest-groups").

A hardcopy, indexed version is available from Prentice Hall under the title *Internet: Mailing Lists* (ISBN 0-13-327941-3).

#### The USENET lists of newsgroups and mailing lists

David Lawrence maintains two lists of newsgroups on Usenet. The "List of Active Newsgroups" lists the regular Usenet newsgroups. The Usenet software also allows the transport of hierarchies of newsgroups not part of the "traditional" Usenet (bionet, alt-groups, bit.listserv etc.). These groups are listed in the list of "Alternative Newsgroup Hierarchies". Both lists contain one line descriptions.

Stephanie da Silva maintains the list of "Publicly Accessible Mailing Lists". This is a list of mailing lists available primarily through the Internet and the UUCP network. The list includes short descriptions of the purpose of the lists.

These lists are distributed via the Usenet newsgroups news.lists and news.answers (monthly updates). News.answers is archived at many sites. The files are named "active-newsgroups", "alt-hierarchies" and "mailing-lists". They can also be obtained from the MIT Usenet archive: by anonymous ftp from rtfm.mit.edu in "/pub/usenet/news.answers" or via email from "mail-server@rtfm.mit.edu". The appropriate commands are:

send usenet/news.answers/active-newsgroups/\*

send usenet/news.answers/alt-hierarchies/\*

send usenet/news.answers/mail/mailling-lists/~

### The Dartmouth SIGLIST

David Avery from Dartmouth maintains a combined edited list (over 500 KB!) of Listserved and manually maintained lists on both Bitnet and Internet. The list includes short descriptions of the purpose of the lists and is sorted by category (computing, science, humanities etc.). It is updated monthly. Dartmouth provides several versions of the list. They also provide several applications (MacIntosh Hypercard, MSDOS, VM/CMS, VAX/VMS and Unix) that present the list in a nice format and facilitate searches.

SIGLIST is available:

-- by anonymous ftp from DARTCMS1.DARTMOUTH.EDU in directory  
SIGLISTS.

-- by email from LISTSERV@DARTCMS1.BITNET ("INDEX SIGLISTS" for a list  
of files and "GET READ ME" for more information )

### The "Directory of Scholarly Electronic Conferences" (ACADLIST)

From the README file: "This directory contains descriptions of electronic conferences (e-conferences) on topics of interest to scholars. E-conference is the umbrella term that includes discussion lists, interest groups, e-journals, e-newsletters, Usenet newsgroups, forums, etc. We have used our own judgment in deciding what is of scholarly interest, and accept any advice or argument about our decisions."

ACADLIST (from Kent State University) is an annotated list. The entries are placed into categories according to the academic subject area of the e-conference. ACADLIST consists of 8 separate text files. Please note that the first four files contain several subject areas arranged in alphabetical order. FILE1 is titled: "Anthropology-Education", this means that it contains all the subject areas that fall alphabetically between A and E! The list is also available as a two file HYPERCARD stack and as a one file MS WORD document (MAC version!).

ACADLIST is available:

-- by anonymous ftp from KSUVXA.KENT.EDU in the directory "library" (get  
"acadlist.readme" for more information).

-- by email from LISTSERV@KENTVM.BITNET ("GET ACADLIST README"

for more information).

## NEW-LIST

The NEW-LIST mailing list at [LISTSERV@NDSUVM1.BITNET](mailto:LISTSERV@NDSUVM1.BITNET) provides announcements of new mailing lists. To subscribe send the command "SUB NEW-LIST Yourfirstname Yourlastname" to the [LISTSERV](mailto:LISTSERV). The mailing list is gatewayed to Usenet as the newsgroup "bit.listserv.new-list". The NEW-LIST archive is the principal source for list searches. It contains three databases in a searchable format:

- lists:       the [LISTSERV](mailto:LISTSERV) list of lists
- intgroup:   the Internet "interest-groups" list
- new-list:   the archived contributions to the NEW-LIST mailing list.

From Marty Hoag's "Some lists of lists":

For example, to search of both these databases for lists on "bicycles" you would send the statements

```
//DBlook JOB Echo=No
Database Search DD=Rules
//Rules DD *
Select bicycle in lists
index
Select bicycle in intgroup
index
Select bicycle in new-list
index
/*
```

in the text/body of the mail to [LISTSERV@VM1.NoDak.EDU](mailto:LISTSERV@VM1.NoDak.EDU) or on BITNET just [LISTSERV@NDSUVM1](mailto:LISTSERV@NDSUVM1). These statements would search the global [LISTSERV](mailto:LISTSERV) list of lists ("in lists"), and the local copy of the SRI-NIC Interest Groups ("in intgroup"), and the archives of the "new-list" list ("in new-list")."

To get more information subsequently submit the following job (substitute "list-number(s)" by the numbers of the lists of interest found in the first job, separated by spaces):

```
// JOB Echo=No
Database Search DD=Rules
//Rules DD *
Select bicycle in lists
```



```

index
print list-number(s)
Select bicycle in intgroup
index
print list-number(s)
Select bicycle in new-list
index
print list-number(s)
/*

```

Send LISTSERV the command INFO DATABASE for more information.

### LIST SEARCHES ON THE INTERNET

Many sites provide a searchable version of one or more lists of lists via gopher. To find them, connect via gopher to a Veronica-server (usually, you'll get there by choosing something like "Other gopher and information servers" in your main menu) and search for "-t7 list lists" "-t7 mailing lists" and/or "-t7 interest groups". The "-t7" addition assures that you'll get searchable versions only. A search for "list lists" will give you about 20 links, "interest groups" about 30, "mailing lists" more than 100, and "lists" more than 4,000. However, this method has several drawbacks. The most important one is that you can never be sure that the lists are regularly updated. There are sites that provide a version of February 1992! Another is that many of those links point to the ghosts of once existing databases (e.g. to lists.src or mailing-lists.src). The Lund University Library Services (Sweden) provides a searchable WAIS-based version of ACADLIST ("academic email conf.src"). There are several ways to access this database:

- By means of your own WAIS client
- There are more than 60 gophers linked to this database (use Veronica to find one).
- Several gopher sites provide a general gateway to WAIS (e.g. the gopherhome in Minnesota).
- Telnet to one of the following servers: quake.think.com (login: wais), nnsf.net (login: wais), swais.cwis.uci.edu (login: swais), sunsite.unc.edu (login: swais), or info.funet.fi (login: info)

### ADDITION (15 May 1993)

The Association of Research Libraries publishes a hardcopy "Directory of Electronic Journals, Newsletters and Academic Discussion Lists" (ISSN: 1057-1337) edited by Diana Kovacs and Michael Strangelove. This directory is derived from network-accessible files. The section on scholarly discussion lists and interest groups is derived from ACADLIST mentioned above. The section on journals and newsletters is derived from Strangelove's "Directory of Electronic Journals and Newsletters". This directory is available from several

sources, e.g. from `LISTSERV@UOTTAWA.BITNET` by sending the commands "get Ejournl1 Directory" and "get Ejournl2 Directory". To order the ARL directory contact Gloria Haws, Publications Manager of the Association of Research Libraries, email: `osap@cni.org`. The price of one copy is USD 42 plus postage, shipping and handling charges.

## APPENDIX F-1

### Expeditionary Environment Research & Analysis Framework & Model 1990

#### EXPEDITIONARY ENVIRONMENT RESEARCH & ANALYSIS FRAMEWORK & MODEL 1990 (DRAFT CONCEPT UNDER DEVELOPMENT)

USMC INTELLIGENCE CENTER  
MARINE CORPS COMBAT DEVELOPMENT COMMAND  
QUANTICO, VIRGINIA  
(703) 640-3177/2268 GRAY 980-6109/10

#### CONTENTS

Brief.....	Tab A
Military Capabilities.....	Tab B
Operational Geography.....	Tab C
Civil Factors.....	Tab D
Insurgency Template & Framework Application.....	Tab E

21 MAY 1990

**OBJECTIVES & PURPOSE OF THE MODEL & SUPPORTING FRAMEWORK**

- TO DEVELOP A GENERIC THREAT MODEL USEFUL TO MARINE CORPS PLANNERS & PROGRAMMERS USING THE CONCEPT BASED REQUIREMENTS SYSTEM (CBRS)
- TO DEVELOP A VALIDATED ANALYTICAL FRAMEWORK WHICH IDENTIFIES "CENTERS OF GRAVITY" AND KEY PLANNING & PROGRAMMING FACTORS ABOUT MILITARY CAPABILITIES AND PHYSICAL & HUMAN CONDITIONS AGAINST WHICH INTELLIGENCE ASSESSMENTS SHOULD BE DEVELOPED.
- SET THE STAGE FOR APPLYING THE FRAMEWORK TO COUNTRIES OF INTEREST TO THE MARINE CORPS IN ORDER TO DEVELOP A GENERIC UNCLASSIFIED INTELLIGENCE MODEL OF WHAT CAPABILITIES AND CONDITIONS WILL BE ENCOUNTERED BY THE MARINE CORPS IN THEIR MOST LIKELY AREAS OF OPERATION.

JUSTIFICATION FOR DEVELOPMENT OF A GENERIC FRAMEWORK

- USE OF THE SOVIET/WARSAW PACT AS THE ONLY "WORST-CASE" SCENARIO IS NO LONGER ACCEPTABLE
- THERE ARE ALTERNATIVE "WORST CASE" SCENARIOS IN THE THIRD WORLD WHICH MUST BE CONSIDERED
- IT IS NOT POSSIBLE TO DEVELOP A DETAILED REVIEW OF ALL COUNTRIES, OR ALL THIRD WORLD COUNTRIES, FOR EACH CBRB REQUIREMENT
- WHAT IS NEEDED IS A GENERIC MODEL BASED ON INTELLIGENCE ABOUT FACTORS WHICH PLANNERS & PROGRAMMERS HAVE IDENTIFIED AS IMPORTANT, AND IS:
  - BASED ON COUNTRY-SPECIFIC REVIEWS FROM WHICH GENERALIZATIONS USEFUL TO CBRB CAN BE DRAWN;
  - SPECIFIC ENOUGH AT THE UNCLASSIFIED LEVEL TO ENABLE PLANNERS & PROGRAMMERS TO DO ESTIMATES OR EVALUATIONS OF REQUIRED OPERATIONAL CAPABILITIES
  - GENERAL ENOUGH SO THAT DETAILED & CLASSIFIED COUNTRY-SPECIFIC TECHNICAL ANALYSIS CAN "FIT" INTO AN OVER-ALL PACKAGE USEFUL TO MISSION AREA PLANNERS & PROGRAMMERS

EXPEDITIONARY ENVIRONMENT RESEARCH & ANALYSIS FRAMEWORK 1990

CONDITIONS & CAPABILITIES	HIGH	MEDIUM	LOW
MILITARY CAPABILITY			
OPS GEOGRAPHY			
CIVIL COMPLEXITY			

- FRAMEWORK DESIGN BASED ON COMBINATION OF NOIC BASELINE FOR NAVAL THREAT, IPB PROCESS, ORIGINAL WORK AND WARFIGHTING CENTER CONCEPTS AND PLANS AND HAA CRITERIA.
- AS ANALYTICAL FRAMEWORK DEVELOPS, MUST DEFINE WHAT IS TO BE MEASURED, HOW ("OBSERVABLES") FACTORS CAN BE MEASURED, AND, BASED ON INPUT FROM PLANNERS & PROGRAMMERS, WHY (JUSTIFICATION) FOR DIVIDING LINES BETWEEN "HIGH", "MEDIUM", AND "LOW" THRESHOLDS FOR EACH FACTOR.
- FRAMEWORK WILL BE VALIDATED THROUGH COUNTRY-SPECIFIC ANALYSIS; VALIDATION WILL LEAD TO SPECIFIC TRUEISMS, GENERIC GENERALITIES, AND DEVELOPMENT OF NEW AND PERHAPS UNANTICIPATED GENERALITIES & SPECIFICS

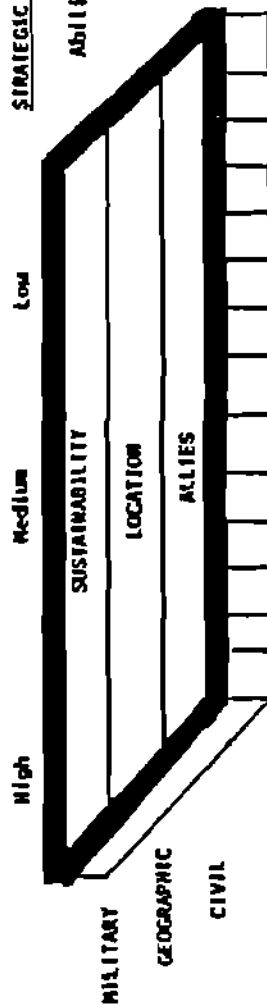
WHAT THE FRAMEWORK DOES NOT DO

- THE FRAMEWORK DOES NOT PROVIDE CLASSIFIED TECHNICAL INTELLIGENCE PERTINENT TO SPECIFIC COUNTRIES, FACTORS, OR SYSTEMS TO BE EVALUATED
- THE FRAMEWORK DOES NOT PROVIDE "NET ASSESSMENTS" (COMPARISONS & JUDGEMENTS OF FRIENDLY VERSUS ENEMY CAPABILITIES & CONSTRAINTS)
- THE FRAMEWORK DOES NOT PRESCRIBE FRIENDLY REQUIREMENTS OR TACTICAL & OPERATIONAL CAPABILITIES TO BE CONSIDERED BY MISSION AREA PLANNERS & PROGRAMMERS
- THE FRAMEWORK IS NOT "FROZEN" AND WILL BE CONSTANTLY REVISED AS COUNTRIES, FACTORS, AND ACTUAL CONDITIONS & CAPABILITIES CHANGE, PROVIDING PLANNERS & PROGRAMMERS WITH A "LIVING DOCUMENT"

# CONCEPT OF OPERATIONS FOR INTEGRATED INTELLIGENCE ANALYSIS

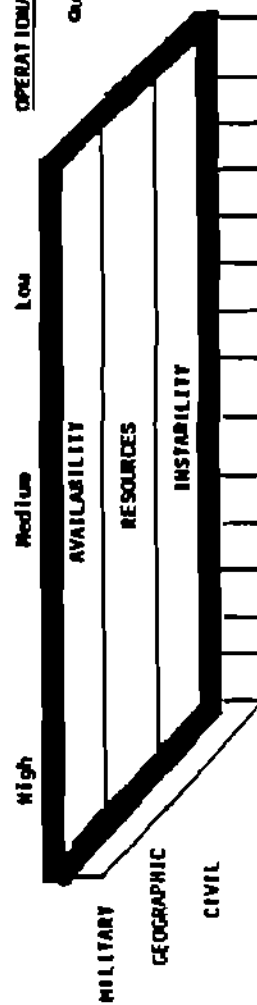
STRATEGIC LEVEL - Integrated Application of all national sources of power

Ability to sustain operations over time & space  
Strategic geo-political location or source of materials  
External relationships of strategic import



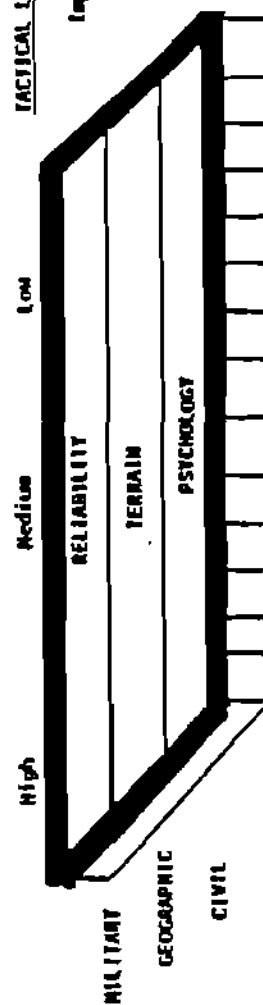
OPERATIONAL LEVEL - Selection of time, space, and nature of engagements

Quantities of military power available for commitment  
Internal natural resources  
Internal precipitants & preconditions of volatility



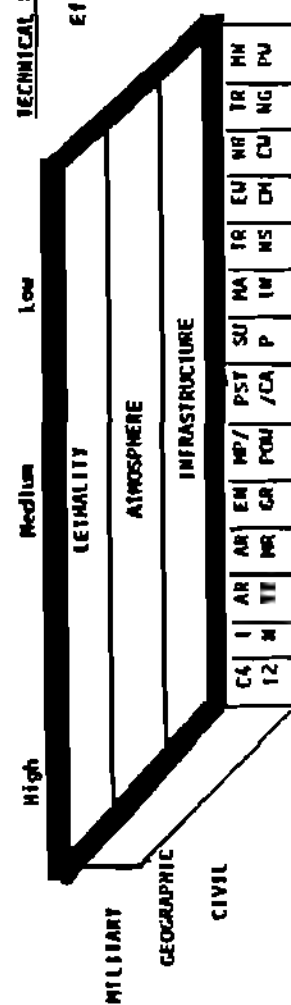
TACTICAL LEVEL - Application of finite power at fixed time & place

Impact of training & maintenance on existing capabilities  
Internal geographic conditions affecting mobility  
Internal group dynamics affecting cohesion & operations



TECHNICAL LEVEL - System-specific capabilities assessed in isolation

Effectiveness of specific capabilities assuming no constraints  
Internal climate affecting system performance  
Civilian structures enabling or blocking system use



MISSION AREA ANALYSIS SLICE - Vertical & Horizontal Looks  
Vertical: through each level of warfare  
Horizontal: in relation to geographic & civil factors



## EXPEDITIONARY ENVIRONMENT - TERMS OF REFERENCE

### Level of Warfare

Strategic.....Integrated application of all national sources of power  
Operational.....Selection of time, space, and nature of tactical engagements  
                    in order to attain strategic objectives - theater level  
Tactical.....Application of finite combat power at fixed time & place  
Technical.....System-specific capabilities independent of external conditions

### Military Capability

Sustainability.....Ability to bring to sustain military operations over time & space  
Availability.....Quantities of military power available for commitment  
Reliability.....Impact of training & maintenance on existing capabilities  
Lethality.....Effectiveness of specific capabilities assuming no constraints

### Geographic Condition

Location.....Strategic geo-political location or source of minerals  
Resources.....Internal natural resources affording self-sustainment  
Terrain.....Internal geographic conditions affecting mobility  
Atmosphere.....Internal atmospheric conditions affecting system performance

### Civil Complexity

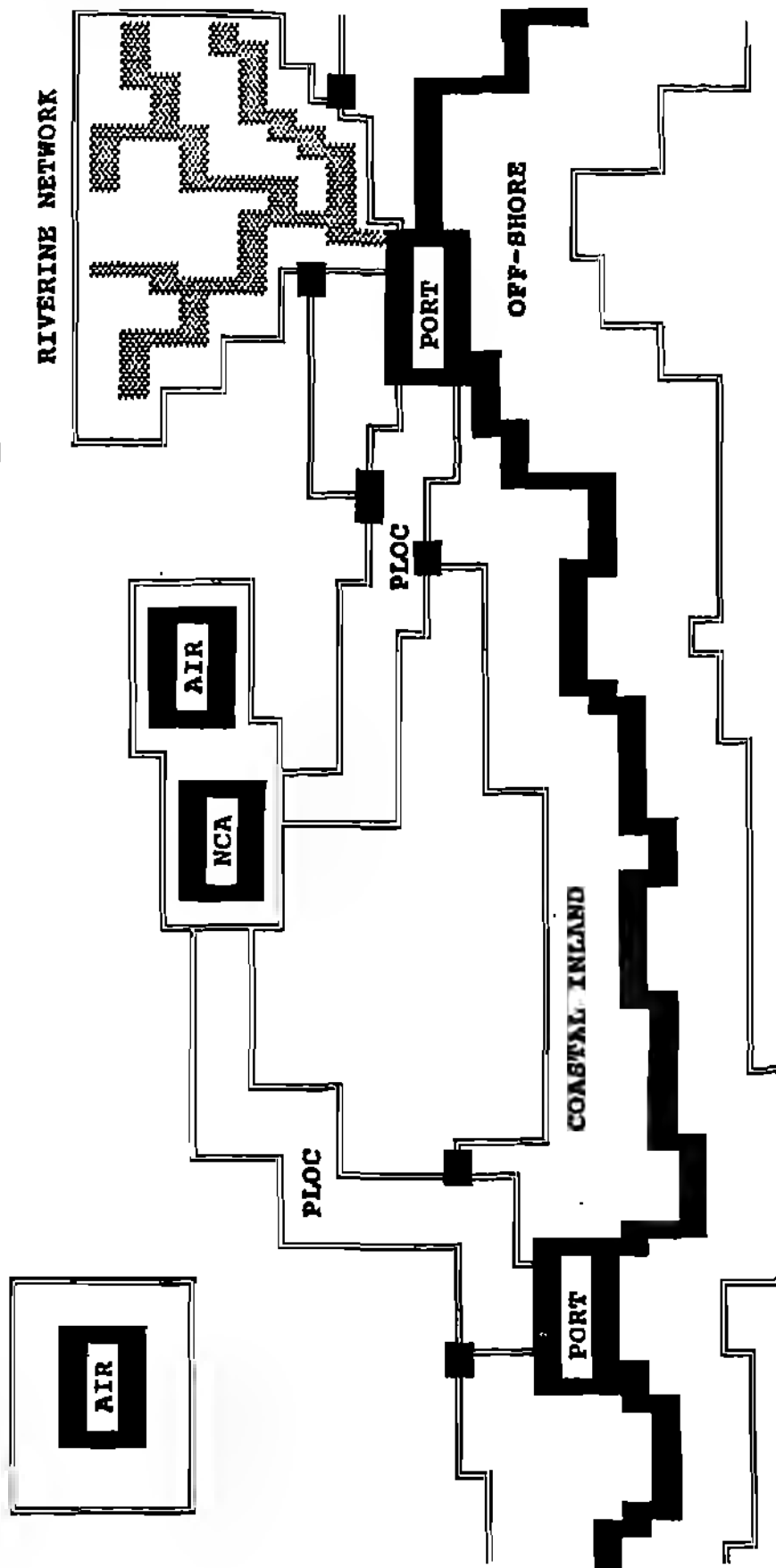
Allies.....External relationships of strategic importance  
Instability.....Internal conditions affecting regime/insurgent effectiveness  
Psychology.....Internal group dynamics affecting national cohesion  
Infrastructure.....Internal structures affecting national capabilities

### Areas of Operation

Off-Shore.....From 25 NM off-shore to high-water mark  
Inland Coast.....From high-water mark to 50 K inland  
PLOC.....Primary Line of Communication from Port to NCA + 30 K each side  
NCA.....National Capital Area + nearest strategic airhead + 30 K around  
Internal.....Riverine networks, other concentrations of people, military, or  
                    key infrastructure nodes

# ILLUSTRATION OF EXPEDITIONARY AREAS OF OPERATION

(Method of Delimiting Analysis Problem)



OFF-SHORE:  
COASTAL INLAND:  
PLOC:  
NCA:  
INTERNAL:

25 NM TO HIGH-WATER MARK  
HIGH-WATER MARK TO 50 K INLAND  
PRIMARY LINE OF COMMUNICATION FROM PORT TO NCA + 30 K EACH SIDE  
NATIONAL CAPITAL AREA + NEAREST STRATEGIC AIR HEAD + 30 K ALL ROUND  
RIVERINE NETWORKS, OTHER STRATEGIC AIR HEADS OR CONCENTRATIONS OF  
PEOPLE, MILITARY, OR KEY INFRASTRUCTURE NODES

**EXPEDITIONARY ENVIRONMENT RESEARCH & ANALYSIS FRAMEWORK 1990**  
**(Early Generalizations)**

CONDITIONS & CAPABILITIES	HIGH	MEDIUM	LOW
<b>MILITARY CAPABILITY</b>	Fully integrated high-tech military infrastructure with mobile deep-strike capabilities incl atk air, arty, & BSM followed by mech combined arms force capable of sustained ops	Defined military infrastructure with emerging air-ground strategy. Capable of uncoordinated air & ground attacks, hasty & deliberate defenses, limited reinforcements, withdrawal/delay	Fragmented military infrastructure based on old or poorly defined technologies. Capable of hasty defenses and delaying tactics.
<b>OPERATIONAL GEOGRAPHY</b>	Trails, dirt roads in highly forested mountain region over 9000 ft, snowing, temperature below freezing, visibility less than 1000 M	Constrained landing sites, single egress to single land roads in rolling hills w/ scattered trees, to small city. Airfield avail for tacops	Airfield suitable for strategic air transport, rural plain, 40 ft draft port with multiple cranes, piers, and electric power
<b>CIVIL COMPLEXITY</b>	Regional power with allies, fanatical religion, strong international media and propaganda capability, global intel organization, independent energy/food	Garrison state with grass roots support or fragmented un-armed opposition, major urbanization, widespread disease or famine, sufficient water, food, energy	Rural/urban opposition w/local base, limited nat'l intel capability, small elite w/o mass apt, urban/rural mix, no safehaven

NEXT STEPS IN THE DEVELOPMENT OF THE GENERIC FRAMEWORK

- USMC INTELLIGENCE CENTER MUST INITIALLY APPLY ROUGH FRAMEWORK WHICH NOW EXISTS TO A SINGLE COUNTRY TO DETERMINE:
  - AVAILABILITY & RELIABILITY OF INFORMATION
  - RELEVANCE OF CHOSEN CRITERIA
  - IDENTIFICATION OF ADDITIONAL OR ALTERNATIVE CRITERIA
- REFINE FRAMEWORK BASED ON COUNTRY-SPECIFIC ANALYSES.
- DO SUFFICIENT INTERACTIONS TO ESTABLISH REPETITIVE PATTERNS AND VALID GENERALIZATIONS.
- RESULTS WILL ESTABLISH "ACCEPTABLE GENERALITIES" WHICH WILL DEFINE THE EXPEDITIONARY ENVIRONMENT MODEL WHILE ACCOMODATING REGIONAL DISTINCTIONS AND COUNTRY-UNIQUE CONDITIONS.

PROCESS FOR DELPHIC USE OF RESEARCH & ANALYSIS FRAMEWORK

FACTOR	HIGH	MEDIUM	LOW
ARTILLERY	SP or towed, with rockets & missiles, NBC, range 30K+	SP or towed, with some missiles, bio-chem, <30K range	Towed artillery with <30K range and/or mortars
MOUNTAINS	High steep slope range with heavy trees cover or low range w/o cover	Low mountain range with scattered trees	Small rolling hills with light scattered trees
OPPOSITION - ORGANIZED - POPULAR	International Opposition with Popular Sympathy	National Opposition with Grass Roots Spt	Rural or Urban Opposition with Only Local Base

- Discuss each factor & description
- Refine descriptions to distinguish between levels
- Categorize level of country for each factor
- Provide one or two bullets justifying each categorization
- Identify an "observable" for each bullet
- Identify data base or data source for each observable
- Identify collection/processing/production gap if appropriate
- State whether factor is moving higher or lower
- Identify any other factors bearing on categorization

EXAMPLE

**LIBYA: POLITICAL-LEGAL/Opposition**

- Rated both high and low
- High because of Egypt and Chad
- Low because of Islamic fundamentalists but relative control
- Number of incidents or denunciations by Egypt & Chad can be plotted
- Public references to Islamic fundamentalists can be plotted
- Need automated scanning/extraction of open source print/voice media
- Need improved clandestine HUMINT reporting as well as emigre debriefing

## MILITARY CAPABILITIES SHAPING THE EXPEDITIONARY ENVIRONMENT

### Executive Summary

- Military capabilities shaping the expeditionary environment should be considered in each of five dimensions:
  - Ground Overview
  - C4I2
  - Combat Support
  - Combat Service Support
  - Readiness & Other Factors
  - Military Manning
  - Aviation Overview (2)
  - EW
  - NBC
- The threat within each dimension can be related to the lethality, range, effectiveness, and sustainability of each capability. For this reason some of the capabilities (e.g. combat arms) will depend on the degree to which other capabilities (e.g. training) are present.
- Examples of a "high", "medium", and "low" environment:
  - High: A fully integrated high-tech military infrastructure based on an air-ground combined arms strategy utilizing state-of-the-art technologies. Envision a highly mobile, deep-strike capability utilizing ground attack aircraft, long range artillery or SSM's deploying non-persistent CW agents followed by a mechanized combined arms ground force attack to quickly neutralize and destroy opposing forces.
  - Medium: A defined military infrastructure with an emerging air-ground strategy utilizing current technologies but attempting high-tech systems integration. Envision an enemy capable of uncoordinated air and ground attacks, hasty and deliberate defenses, limited reinforcements, withdrawal and delaying tactics.
  - Low: A fragmented military infrastructure with segregated military capabilities based on obsolete or ill-defined technologies. Envision an enemy capable of hasty defense and delaying tactics only.

# OVERVIEW OF GROUND FACTORS SHAPING THE EXPEDITIONARY ENVIRONMENT

CAPABILITY	HIGH	MEDIUM	LOW
INFANTRY	Mechanized, division-sized combined arms capable with ALP	Mobile trained Rgts or Bns with some combined arms	Bn-sized forces with limited mobility & spt
ARTILLERY	SP or towed, with rockets & missiles, NBC, range 30K+	SP or towed, with some missiles, biochem, <30K range	Towed artillery with <30K range and/or mortars
ARMOR	T-72MI or T-80/64B equivalent with advanced armor (R/A)	M-60, T-62E/Mod 55 equivalent with 3rd gen. armor	M-48/T-54/IFV equivalents or lead
C4I2	Integrated strategic & tactical C4I2 using full RF spectrum	Terrestrial RF and landlines, limited encryption & intel	Single-channel radio, limited encryption/intel
SUPPORT	Full-range engineers, complete military police/PSYOP-CA units,	Limited engineers, some military police and PSYOP-CA	Counter mobility engineering, no dedicated MP/PSYOP
SERVICE SUPPORT	Able to move, supply, & maintain a division beyond its borders	Can move, supply, & maintain rgmts & bns within borders	Some resupply & limited maint. capability
LEADERSHIP, TRAINING, & READINESS	Corps+ leaders, troops experienced, well-trained, fully ready	Div level leaders, some troop training partially ready	Regt lev leaders, no or infrequent training, not rdy
MILITARY MANNING	Foreign advisors, full reserve, PM/elite units	Foreign contractors, partial reserves, some PM/elite units	Constabulary or pro forma reserve w/o SOF

**C4I2 FACTORS SHAPING THE EXPEDITIONARY ENVIRONMENT**

<b>CAPABILITY</b>	<b>HIGH</b>	<b>MEDIUM</b>	<b>LOW</b>
<b>COMMAND &amp; CONTROL &amp; COMMUNICATIONS</b>	Integrated automated C4 btw NCA & ground/ air hqs; national/alt. CP, full RF & SATCOM, encryption all levels	Limited C4 automation w/reliance on land- lines & terrestrial RF w/strategic encryp- tion, tac. ops codes	No integration or automation of C4, use single channel radios (e.g. HF), offline encry/clear
<b>COMPUTING</b>	Mainframe & high performance distributed processing, ADP tools	Limited use of stand alone workstations, basic PC packages	Manual data process- ing and report production
<b>INTELLIGENCE &amp; INTEROPERABILITY</b>	Multi-discipline collection capability w/all-source analysis at national & tactical levels	Strategic intel from allies, some SIGINT, IMINT, HUMINT collec- tion, limited inte- gration	Limited strategic intel from allies, national HUMINT, tactical SIGINT, no/ limited IMINT



COMBAT SUPPORT FACTORS SHAPING THE EXPEDITIONARY ENVIRONMENT

CAPABILITY	HIGH	MEDIUM	LOW
ANTI-TANK	FGM, atk helo, self-propelled AT, arty/air deliverable mines	SP AT, RR, arty/air deliverable mines	Crew served or shoulder launched AT weapons
ENGINEERS	Heavy equipment, can do mobility/countermobility, survivability, gen eng.	Few heavy assets, can do minefields & obstacles, demolit.	Manual minefield & obstacle construction & clearing
MILITARY POLICE	Dedicated organized MP units able to handle mass refugee/POW groups	Limited organized MP units able to handle routine matters	No dedicated MP units; law enforcement by infantry
PSYOP & CIVIL AFFAIRS	Dedicated organized PSYOP/CA units with organic equipment	Limited organized PSYOP/CA specialists detailed to infantry	No organized PSYOP or CA capabilities

COMBAT SERVICE SUPPORT FACTORS SHAPING THE EXPEDITIONARY ENVIRONMENT

CAPABILITY	HIGH	MEDIUM	LOW
SUPPLY	Self-sufficient, can sustain combat ops for over 6 months, to include external ops	Self-sustaining up to 6 months, rely on allies for supplies	Self-sustaining for less than 30 days, rely on allies/raids
MAINTENANCE	Unit, intermediate, & depot-level	Unit & intermediate (DS & GS units), external depot spt	Unit level only. Dependent on external manning & facilities
TRANSPORTATION	Modern assets, fast response, not reliant on commercial assets	Good rail & roads, limited air, partial use of commercial	Primitive or limited transport, slow response, commercial

READINESS & OTHER FACTORS SHAPING THE EXPEDITIONARY ENVIRONMENT

CAPABILITY	HIGH	MEDIUM	LOW
LEADERSHIP	Combat experience, Corps-level staffs, professional schools	Ops/exercises done, div-level staffs, few foreign advisors	Regiment-level staffs, rely on foreign advisors
TRAINING	Training at division level or higher, 3-5 days per month	Training at Rgmt or lower level, 1-3 days per month	Infrequent training at/below 1 day per month
READINESS	All equipment receives preventive maintenance from trained personnel	Most equipment in ready status, is repaired as needed	Generally poor maintenance, most equipment deficient

# **MILITARY MANNING FACTORS SHAPING THE EXPEDITIONARY ENVIRONMENT**

<b>CAPABILITY</b>	<b>HIGH</b>	<b>MEDIUM</b>	<b>LOW</b>
<b>FOREIGN ADVISORS</b>	In-country, providing R&D or intel support, of manning equipment	Intel & operational advisory role, MTTs, liaison/oversight	Temporary travel in-country for MTT or supply purposes
<b>CONTRACTORS</b>	Fully responsible for manning and/or maint. of critical systems	Responsible for maintenance & testing of key systems	Temporary travel in-country for installation/repair
<b>RESERVES</b>	Organized trained reserve able to fill range of combat needs	Organized coastal, constabulary, or specialty units	No organized units or regular training
<b>PM/SOF/ELITE</b>	Trained & specially equipped units with unique status	Organized units with special roles and loyalties	No organized PM, SOF, or elite units

# OVERVIEW OF AVIATION FACTORS SHAPING THE EXPEDITIONARY ENVIRONMENT

CAPABILITY	HIGH	MEDIUM	LOW
AIR SURVEILLANCE WEAPONS SUPPORT	Full integrated air defense net, with digital automation	2nd/3rd generation Soviet/Western IAD	Limited IAD netting with landline links
FIGHTER AIRCRAFT (FIXED & VSTOL)	4th generation Soviet / Western full LD/SD capability	3rd generation Soviet /Western limited LD/SD cap	Early jets with limited scramble, no sustained CAP
STRIKE AIRCRAFT (FIXED & VSTOL)	All-weather medium & long-range, NBC capable	Marginal all-weather medium/long range without NBC	Day only, VFR delivery
HELICOPTERS (BOTH ATTACK & TRANSPORT)	4th gen. attack & transport	3rd gen. attack & transport, limited assets	No military assets, limited commercial assets
SURFACE TO AIR MISSILES	4th Gen Soviet/Western Strategic / Tactical Improved IR	3rd Gen Soviet/West Strategic/Tactical	Hand Held Tactical IR Only
ANTI-AIRCRAFT ARTILLERY	4th Gen Soviet/West Radar associated Mobile	3rd Gen Soviet/West limited radar restricted mobile	Small arms Optical sighting Manual operations
AIR TO AIR MISSILES	4th Gen Soviet/West Dual Mode True All-Aspect	3rd Gen Soviet/West Limited All-Aspect	Early IR/SAR Rear Quarter

OVERVIEW OF AVIATION FACTORS SHAPING THE EXPEDITIONARY ENVIRONMENT

CAPABILITY	HIGH	MEDIUM	LOW
RECONNAISSANCE	Long-range dedicated platform with real-time links	Medium/long-range multi-role platform w/NRT links	Low mission priority with no NRT links
AIRBORNE EARLY WARNING/CONTROLLER (AEW)	Long-range/extended loiter time, multi-mission, digital links	Single mission ops w/limited coverage, voice links	No capability
TACTICAL ELECTRONIC WARFARE (TACEW)	Dedicated platform ESM/ECH, both fixed wing & rotor	Self-protection only or helo platforms only for ECH	No capability
TRAINING & READINESS	Simulators, live fire & free play; sustain support all levels	Limited training & live fire; foreign support at depot	Less than 10 hours flight/month; rely on foreign support

**NBC FACTORS SHAPING THE EXPEDITIONARY ENVIRONMENT**

<b>CAPABILITY</b>	<b>HIGH</b>	<b>MEDIUM</b>	<b>LOW</b>
<b>NUCLEAR</b>	Stockpiled nuclear weapons or proven capability to build	Advanced R&D effort, component acquisition, prototypes	No nuclear capability or capacity to develop
<b>CHEMICAL</b>	Indigenous production, full spectrum, prior utilization	Stockpiles of major agent, indigenous or foreign production	Foreign procurement, non-persistent, limited stocks
<b>BIOLOGICAL</b>	Indigenous production, full spectrum of toxic & infectious agents	Microbiology R&D, some infectious agents in stock	Foreign procurement would be needed, no agents in stock
<b>DELIVERY</b>	Full range of air & missile/artillery delivery systems	Artillery & mortar delivery, some air (rotary) delivery	No tested delivery system

**EW FACTORS SHAPING THE EXPEDITIONARY ENVIRONMENT**

<b>CAPABILITY</b>	<b>HIGH</b>	<b>MEDIUM</b>	<b>LOW</b>
<b>EW SUPPORT MEASURES (ESM)</b>	Automated netted COMINT & ELINT w/DF, capable against full spectrum & w/full proc/rpt	Manual collection & DF against some comms & non-comms signals	Limited or no collection
<b>ELECTRONIC COUNTER MEASURES (ECM)</b>	Mobile programmable jamming/deception, full spectrum, active & passive, varied tech.	Capable of jamming & deception within specific frequency ranges	Limited or no jamming/deception capability (can do ICD obvious jamming)
<b>ELECTRONIC COUNTER-COUNTER MEASURES (ECCH)</b>	Fully developed and exercised system of preventive & remedial measures/equipment	Some doctrine & equipment	Non-existent system or limited to operator training



## OPERATIONAL GEOGRAPHY SHAPING THE EXPEDITIONARY ENVIRONMENT

### Executive Summary

- Operational geography shaping the expeditionary environment should be considered in each of six dimensions:
  - Basic Topography                      -- Ground Assault Conditions
  - Assault Hydrography                -- Aeronautical Conditions
  - Operational Infrastructure        -- Basic Weather
- The threat within each dimension can be related to the degree to which topographical and/or weather conditions constrain operational mobility, firepower, and/or sustainability.
- Examples of a "high", "medium", and "low" environment for these factors is offered below:
  - High: Trails, dirt roads in a highly forested mountain region over 9000 ft, snowing, temperature at 0, visibility less than 1000 meters, with objective too far inland to permit sea-launched assault and naval gunfire support.
  - Medium: Single amphibious landing vehicle sites with egress to single lane hard surface roads and rail roads, small rolling hills with moderate scattered trees, to a small city. Airfield suitable for sustained tactical air transport operations.
  - Low: Airfield suitable for sustained strategic air transport. Rural plain, 40 ft draft port facility that has multiple cranes, piers and electric power.

OPERATIONAL GEOGRAPHY SHAPING THE EXPEDITIONARY ENVIRONMENT

BASIC TOPOGRAPHY	GROUND ASSAULT	ASSAULT HYDROGRAPHY	AERONAUTICAL CONDITIONS	OPERATIONAL INFRASTRUCTURE	BASIC WEATHER
Surface Configuration	Cover	Beaches	Ops Elevation	Port Access	Temperat.
Surface Vegetation	Concealment	NGF (5 fathom line)	Aerial Visibility	Port Utility	Windspeed
Surface Materials	Inter- visibility	Surf Conditions	Aerial Ceiling	Air Terminals	Precipit.
Surface Hydrology	Landing Zones	Approach Conditions		Road/Rail Net	Humidity
Man-made Features	Drop Zones	Riverine Network		Bridges	Light Data

# BASIC TOPOGRAPHY FACTORS SHAPING THE EXPEDITIONARY ENVIRONMENT

CONDITION	HIGH COMPLEXITY	MEDIUM COMPLEXITY	LOW COMPLEXITY
SURFACE CONFIGURATION	High steep slopes of >40%, ranges with ravines & embankments	Low ranges with small ditches and scattered outcrops	Small rolling hills with valleys and flat areas
SURFACE VEGETATION	Double & triple canopy with heavy dense trees and dense undergrowth	Single canopy with mix of vegetation and open bare ground	Shrubs & grasses on flat plains including cactus or eleph. gr.
SURFACE MATERIALS	Wet clay, silt, large gravel or drifting loose sand, sebkhas & wadis	Moist sand, small gravel or loose unsettled sand	Dry silt, clay, small gravel or flat hard plain w/o sebkhas
SURFACE HYDROLOGY	Lakes, swamps, rivers, and/or glaciers; boats required for crossings	Streams, canals, small rivers; fording equipment needed	Seasonal streams, creeks, no major water obstacles
MANMADE FEATURES	Urban areas, major oil fields, major bridges or tunnels/pipelines	Suburban or village areas, minor power facilities, bridges	Predominantly rural, minor bridges and/or tunnels, few obstacles

GROUND ASSAULT CONDITIONS SHAPING THE EXPEDITIONARY ENVIRONMENT

CONDITION	HIGH COMPLEXITY	MEDIUM COMPLEXITY	LOW COMPLEXITY
COVER	Flat plains and wide open areas	Moderate scattered trees on rolling hills	Densely wooded areas within low mountain range
CONCEALMENT	75% or more canopy closure	40-74% canopy closure	0-39% canopy closure
INTER-VISIBILITY	Average line of sight distance in AO is less than 1000 meters	Average line of sight in AO is 1000 to 3000 meters	Average line of sight in AO is over 3000 meters
LANDING ZONES	Slope of available LZ/HLZ greater than five degrees	Slope of available LZ/HLZ 3-5 degrees	Slope of available LZ/HLZ <3 degrees
DROP ZONES	Few or very small clearings with no ground access/exits	Small playing field size clearings with limited exits	Large open fields with many exits & access to LOCs

# ASSAULT HYDROGRAPHY CONDITIONS SHAPING THE EXPEDITIONARY ENVIRONMENT

CONDITION	HIGH COMPLEXITY	MEDIUM COMPLEXITY	LOW COMPLEXITY
BEACHES	Limited or not avail, with restricted or channeled egress	Sufficient to allow single LCAC or few LAV, multiple egress	Multiple sites for full LAV waves, multiple egress
NAVAL GUN FIRE	5 fathom line more than 16K meters offshore	5 fathom line is >8K <16K meters offshore	5 fathom line is less than 8K meters offshore
SURF CONDITIONS	>3.5 ft. swells, >4.0 ft. surf, underlying current >3 kts	2-3 ft. swells, 2-4 ft. surf, under- current 2-3 kts	0-1 ft. swells, 0-1 ft. surf, under- current < 2 kts.
APPROACH CONDITIONS	>15 ft. tidal range, or slope <1:5 and/or silty/muddy bottom	>5' <15' tidal range and/or slope >2:5 <1:10, sand	<5' tidal range, or slope >1:5 and/ or hard bottom
RIVERINE NETWORK	Major river complex with tributaries >6' deep and ocean access	Defined network w/ streams >3' <6' deep, mostly inland	Seasonal streams <3' deep

**AERONAUTICAL CONDITIONS SHAPING THE EXPEDITIONARY ENVIRONMENT**

<b>CONDITION</b>	<b>HIGH COMPLEXITY</b>	<b>MEDIUM COMPLEXITY</b>	<b>LOW COMPLEXITY</b>
<b>ELEVATION</b>	Over 9000 ft	4000-9000 ft	Less than 4000 ft
<b>AERIAL VISIBILITY</b>	Less than 2 NM	>2 <5 NM	Over 5 NM
<b>AERIAL CEILING</b>	Less than 1000 ft	3-5K ft +/-	Over 10K ft +/-

OPERATIONAL INFRASTRUCTURE CONDITIONS SHAPING THE EXPEDITIONARY ENVIRONMENT

CONDITION	HIGH COMPLEXITY	MEDIUM COMPLEXITY	LOW COMPLEXITY
PORT ACCESS	Less than 34' draft (tactical assault)	35-40' draft (gray shipping)	Over 40' draft (black shipping)
PORT UTILITY	No cranes or piers	At least one crane or pier per port	Multiple cranes & piers, electric power available
AIR TERMINALS	Not good for tactical transport ops, no ground control	Suitable for fully loaded tactical transport ops	Suitable for strategic airlift
AIRHEAD UTILITY	One or no ramps	Two to five ramps, some fuel storage and bunker areas	Five or more ramps suitable for C-5, good fuel/ammo site
ROAD/RAIL NETWORK	Trails, dirt roads, very limited or no railroad	Hard surface single lane roads, single track RR	Major highways, extensive RR
BRIDGES	Many primitive or old bridges of low or unknown load bearing	Mix of steel/cement bridges w/load bearing <20 tons	Modern steel & cement bridges with >20 ton capability

**BASIC WEATHER FACTORS SHAPING THE EXPEDITIONARY ENVIRONMENT**

CONDITIONS	HIGH COMPLEXITY	MEDIUM COMPLEXITY	LOW COMPLEXITY
TEMPERATURE	>80 <32 F	32-50 or 65-80 F	51-64 F
WIND SPEED	>30 knots	13-30 knots	<13 knots
PRECIPITATION	1"/hour or 2"/12 hrs; 2" snow/hour or 6" snow/12 hrs	.5-1"/hour or 1"/ 12 hrs; 1-2" snow/ hr or 3-6"/12 hrs	0-.5"/hour or .5"/ 12 hrs; 0-1" snow/hr 0-3"/12 hrs
HUMIDITY	60-100%	31-59%	12-30%
LIGHT DATA	4-6 hrs daylight	6-10 hrs daylight	>10 hrs daylight



## CIVIL FACTORS SHAPING THE EXPEDITIONARY ENVIRONMENT

### Executive Summary

- Civil factors shaping the expeditionary environment should be considered in each of five dimensions:
  - Political
  - Psychological
  - Economic
  - Infrastructure
  - Natural Resources
- The complexity of the factors, increasing the difficulty facing the tactical commander, can be related to the area of influence of each factor: International = HIGH, National = Medium, Local/Urban = LOW.
- The relevance of the factors to expeditionary operations can be established by determining whether the factor must be considered in relation to short-term missions under 7 days (e.g. a NEO), mid-term missions over 7 but under 30 days (e.g. humanitarian assistance) and longer-term missions over 30 days (e.g. internal security).
- Examples of a "high", "medium", and "low" environment for these factors is offered below:
  - High: Regional power with allies, fanatical religion, strong international media and propaganda capability, global intelligence organization, and independent energy & food supplies.
  - Medium: Garrison state with grass roots support or fragmented unarmed opposition, major urbanization, widespread disease or famine, sufficient water, food, energy.
  - Low: Rural/urban opposition with local base, limited national intelligence capability, small elite without mass support, balanced mix of urban & rural populations, secure borders offering no safehaven.

CIVIL FACTORS - TERMS OF REFERENCE

Civil Dimensions

- Political..... Focus on political relationships between groups and individuals, including external allies and internal opposition groups; and on basic capabilities and legal environment maintaining government control of political process.
- Psychological..... Focus on the ideological and cultural nature of the population and the degree to which individual behavior undermines or supports the nation-state. Assesses role of religion & language as divisive or cohesive factors, group divisions & customs, national myths, and other issues associated with individual education & rebellion.
- Economic..... Focus on ability of state to fulfill its functions and allocate resources, with emphasis on the stability of the consumer market, the role of the military as a dominant group, the general strength of the economy, and the degree to which capital is available and research & development sponsored for future economic power.
- Infrastructure..... Focus on the technical and demographic resources of the nation-state including basic issues regarding population distribution, disease, communications, public works, public transportation, and electronic computing resources.
- Natural Resources..... Focus on natural resources including water, food, energy, and mineral wealth, as well as related issues which contribute to conflicts, such as contiguous hostile areas, land tenure practices, and production base constraints.

CIVIL FACTORS SHAPING THE EXPEDITIONARY ENVIRONMENT

POLITICAL	PSYCHOLOGICAL	ECONOMIC	INFRASTRUCTURE	NATURAL RESOURCES
<p> <b>Allies</b>  <hr/> <b>Opposition</b>  <hr/> <b>Intelligence</b>  <hr/> <b>Government</b>  <hr/> <b>Human Rights</b>  <hr/> <b>Public Form, Franchise, &amp; Opinion</b>  <hr/> <b>Legal Codes</b> </p>	<p> <b>Religion &amp; Language</b>  <hr/> <b>Group Divisions, Customs/Taboos</b>  <hr/> <b>Myth/Identity, Media Themes, &amp; View of USA</b>  <hr/> <b>Education</b>  <hr/> <b>Intellectuals</b>  <hr/> <b>Censorship</b>  <hr/> <b>Violence</b> </p>	<p> <b>Strikes &amp; Riots</b>  <hr/> <b>Black Market, Corruption, &amp; Mil/Pol Crime</b>  <hr/> <b>Unemployment &amp; Inflation</b>  <hr/> <b>Basic Civilian Staples/Supply</b>  <hr/> <b>Garrison State</b>  <hr/> <b>Foreign Capital &amp; Capital Flight</b>  <hr/> <b>R&amp;D Program</b> </p>	<p> <b>Key Facilities &amp; No Fire Areas</b>  <hr/> <b>Urbanization &amp; Population Issues</b>  <hr/> <b>Disease &amp; Public Health Resources</b>  <hr/> <b>Public Voice/Print Media &amp; Telecommunications</b>  <hr/> <b>Public Works (Power &amp; Water)</b>  <hr/> <b>Public Transportation Assets</b>  <hr/> <b>Electronic Computing &amp; Storage</b> </p>	<p> <b>Contiguous Hostile Area</b>  <hr/> <b>Water Supply</b>  <hr/> <b>Food Supply</b>  <hr/> <b>Energy Supply</b>  <hr/> <b>Strategic Minerals &amp; Raw Materials</b>  <hr/> <b>Production Base</b>  <hr/> <b>Land Tenure</b> </p>

POLITICAL FACTORS SHAPING THE EXPEDITIONARY ENVIRONMENT

CONDITION	HIGH COMPLEXITY	MEDIUM COMPLEXITY	LOW COMPLEXITY
ALLIES	Major hostile power or several regional powers	Major regional power or scattered minor supporters	No major ally in region nor Sov/PRC interest
OPPOSITION	International	National	Rural or Urban
- ORGANIZED	Opposition with Popular Sympathy	Opposition with Grass Roots Spt	Opposition with Only Local Base
- POPULAR	International	National	Limited
INTELLIGENCE	Intelligence with Global Assets	Intelligence with Rural/Urban Assets	Intelligence with Capital City Base
- STRUCTURED	Fully capable sovereign government	Nationally capable government with limited int'l role	Parochial or unformed state w/limited powers
- PROFESSIONAL	Violent repression w/o oversight of police &/or military	Limited repression w/some political oversight/pressure	Firm commitment to human rights, broad public pressure
GOVERNMENT	Unrestricted citizen base with protected rights	Partial franchise with popular majority	Very restricted elite without majority support
- STRUCTURED	Religious or primitive codes or patron power	Legal or religious codes partially or arbitrariness used	Established legal system with working courts
- RESPONSIVE			
HUMAN RIGHTS			
PUBLIC FRANCHISE			
- OPINION			
- LEGITIMACY			
LEGAL CODES			
- EXISTENCE			
- EFFECTIVE			

\* Includes gender mix and stratification of population by class, race, religion, or religion.

PSYCHOLOGICAL FACTORS SHAPING THE EXPEDITIONARY ENVIRONMENT

CONDITION	HIGH COMPLEXITY	MEDIUM COMPLEXITY	LOW COMPLEXITY
RELIGION & LANGUAGE	Intense national religion or varied opposed religions; "hard" language	Major religion or mass movement with active role; Western language	Western or varied religions of no real influence; Eng/Frnch/Spanish
GROUP DIVISIONS, CUSTOMS, AND TABOOS	Major fragmentation of society with conflicting mores	Major minority element not fully integrated	No significant socio-economic fragmentation
MYTH/IDENTITY, MEDIA THEMES, & VIEW OF USA	Cohesive national myth system, with xenophobic nature	Strong national identity and sense of history	Limited or fragmented myth system/identity
EDUCATION	No public schools and a primitive illiterate public	Partial public education, literate urban population	Public education and literate population
- PUBLIC			
- QUALITY			
INTELLECTUALS	Strong intellectual community firmly committed to state	Isolated community of intellectuals including exiles	Fragmented or unformed community of intellectuals
- EXISTENCE			
- COMMITMENT			
CENSORSHIP	Total censorship of all media and all topics	Censorship of political topics or select groups	Limited or no censorship
- SCOPE			
- DEGREE			
VIOLENCE	Cultural pre-disposition and history of violence	Elite history of unchecked violence	No significant pre-disposition or history
- PRE-DISPOSED			
- EXTENT			

# ECONOMIC FACTORS SHAPING THE EXPEDITIONARY ENVIRONMENT

CONDITION	HIGH COMPLEXITY	MEDIUM COMPLEXITY	LOW COMPLEXITY
REBELLION (RIOTS, STRIKES, DEMONSTRATIONS)	Frequent and sustained public riots & strikes	Occasional violent rebellion or many demonstrations	Limited and generally peace- ful gatherings
BLACK MARKET & CORRUPTION & MIL/POLICE CRIME	Thoroughly corrupt society, bribes for basic transactions	Limited elite corruption, some bribes necessary	Limited elite corruption, no major monopolies
INFLATION & UNEMPLOYMENT - RATE	Rapid rate of inflation and high unemployment	Fluctuating rates of inflation and unemployment	Steady or limited inflation and unemployment
BASIC CIVILIAN STAPLES/SUPPLY - TYPE/EXTENT	Major shortages of basic staples and household items	Shortages of convenience items & minor luxuries	Full range of staples and consumer goods
GARRISON STATE - MONOPOLY - ISOLATED	Dictatorship or entrenched military controlling economy	"Benevolent" or professional military elite	Militia or home guard with limited role
FOREIGN CAPITAL & CAPITAL FLIGHT	Most elite funds withdrawn and no foreign credit	Steady capital flight, high rates of loan interest	Modest capital flight, steady foreign loans
R&D PROGRAM - FUNDED - QUALITY	National R&D program with high-tech goals	Private industry R&D in some areas	No significant R&D program

# INFRASTRUCTURE FACTORS SHAPING THE EXPEDITIONARY ENVIRONMENT

CONDITION	HIGH COMPLEXITY	MEDIUM COMPLEXITY	LOW COMPLEXITY
KEY FACILITIES & NO FIRE AREAS	Regionally important facilities, many no fire areas	Nationally vital facilities, some no fire areas	No major facilities requiring control, minor no fire areas
POPULATION ISSUES - URBANIZATION - DISPLACEMENT	Excessive and unsupportable urbanization	Major urbanization with limited or sporadic services	Balanced mix of urban & rural populations
DISEASE & HEALTH - SCOPE - ADDRESSED	Uncontrolled famine and/or disease such as AIDS/schistosom.	Major disease such as schistosomiasis and public program	No major disease or famine and/or good public plan
PUBLIC COMMS - VOICE/PRINT MEDIA - TELECOMMUNICATION	Int'l media & propaganda, int'l telecommunications	National media and propaganda capability	Primitive media & limited nat'l telecommunications
PUBLIC WORKS - POWER - WATER	No established public works system	Partial public works and/or frequent breakdown	Established and functional public works system
PUBLIC TRANSPORTATION ASSETS	Major transport fleets with int'l infrastructure	Substantial ground transport fleet w/ national network	Some urban assets w/generally poor roads or rails
ELECTRONIC COMPUTING & STORAGE	National network of electronic data entry & management assets	Strong program of data management in primary industry	Limited or old data storage and management tools

NATURAL RESOURCE FACTORS SHAPING THE EXPEDITIONARY ENVIRONMENT

CONDITION	HIGH COMPLEXITY	MEDIUM COMPLEXITY	LOW COMPLEXITY
EXTERNAL THREAT - CONTIGUOUS - MAJOR POWER	Major hostile power on border	Minor or neutral power on border allowing safehaven	Secure borders offering no safehaven
WATER SUPPLY - LOCAL - RELIABLE	Importer of water or scarce water resources	Sufficient natural water for basic needs	Major rivers and lakes with good water works
FOOD SUPPLY - LOCAL - RELIABLE	Importer of basic foods	Nationally self-sufficient in basic foods	International supplier of major edible commodity
ENERGY SUPPLY - LOCAL - RELIABLE	International supplier of oil or electricity	National reserves of energy, partial exploitation	Importer of oil and/or electric power, coal
STRATEGIC MINERALS & RAW MATERIALS	International supplier of major minerals/materials	National reserves of basic minerals and materials	Importer of basic minerals and materials
PRODUCTION BASE - SINGLE/MULTIPLE - EXPLOITED	Over-reliance on single sector and/or weak market	Strong single sector with good distribution	Balanced mix of production (both indus. & agri.)
LAND TENURE - DISTRIBUTED - EFFECTIVE	Well distributed and exploited land holdings	Limited land tenure, strong share-cropping	Restrictive land tenure, serf-like labor conditions



#### "SO WHAT" TEST FOR CIVIL FACTORS

NOTE: Unlike military conditions and operational geography, the relevance of civil factors to normal MAGTF planning & programming activities may not be as apparent. Although the Small Wars Manual and other doctrinal publication recognize the importance of psychological and civil affairs, and the are clearly defined intelligence requirements associated with these functions as well as engineering, motor transport, and so on, the above matrix sought to bring together the various "civil" factors as a means of integrating them in the intelligence estimates process and highlighting the co-equal status of civil factors when planning for stability operations and limited objective operations.

Political

Allies	Potential for intervention and/or mobilization of regional or international opinion
Opposition	Potential of existing groups (both armed and unarmed) for assisting or opposing MARFOR
-----	
Intelligence	Potential of intelligence & security services for assisting or opposing MARFOR operations, both internally and through covert actions & propaganda activities outside the AO (including against domestic U.S. public)
Government	Potential for assisting or opposing MARFOR
-----	
Human Rights	Establishes degree to which individuals have been repressed, and possible need for remedial programs; includes degree to which entrepreneurship present & successful
Franchise	Insights into nature of public's political personality, degree to which public opinion can air or hamper MARFOR and/or government
Legal Codes	Foundation of internal order

## Psychological

**Religion & Language** Degree of difficulty for HARFOR intel, PAO, and engineers; includes religious codes and language conventions which HARFOR must understand

**Group Divisions, Customs/Taboos** Degree to which certain groups must be monitored and HARFOR behavior adjusted

-----

**Myth/Identity, Media Themes, & View of USA** Provides HARFOR with estimate of cohesiveness of population, understanding of popular propaganda themes, and attitudes toward USA

**Education** Establishes degree of popular literacy in relation to HARFOR public information program and public understanding of issues

-----

**Intellectuals** Establishes location & nature of key leaders of public opinion and degree to which they might oppose/support HARFOR ops

**Censorship** Establishes degree to which public has been misinformed, and degree to which HARFOR must undertake remedial public information program

**Violence** Establishes degree to which local population is culturally pre-disposed to violence, and alerts HARFOR to potential volatility

## Economic

Rebellion	Degree to which population supports insurgents and/or might impact HARFOR ops
Black Market, Corruption, & Mil/Pol Crime	Orients HARFOR to local "norms" (including need for HARFOR discretionary funds) as well as general dislocation of economy and degree to which local forces are regarded as "predators"
-----	
Inflation & Unemployment	Degree to which economic dislocation exists that may interfere with long-term HARFOR ops
Basic Civilian Staples/Supply	Degree to which civilians lack staples for diet or consumer goods which HARFOR must provide, or which HARFOR can draw upon in lieu of external resupply
-----	
Garrison State	Degree to which AO is militarized
Foreign Capital & Capital Flight	Presence or absence of foreign equities and/or flight of internal capital may complicate conditions for HARFOR
R&D Program	Identifies degree to which military R&D might threaten HARFOR, and general health of local R&D effort as it supports prosperity

## Infrastructure

### Key Facilities & No Fire Areas

Identifies key facilities requiring MARFOR protection and possibly operation, and key sites (archives, monuments, etcetera) that constrain MARFOR ops

### Population Issues

Establishes concentrations of people that MARFOR must deal with, and potential for displaced persons, refugees, and groups requiring MARFOR control or support

### Disease & Public Health Resources

Identifies major diseases dangerous to individual Marines, degree to which local health resources are present or absent, extent to which MARFOR must provide medical reinforcements

### Public Comms (Voice/Print Media & Telecomms)

Identifies degree to which existing local media outlets can be mobilized to meet MARFOR public information requirements; also availability of commercial telecommunications to be controlled, monitored, or exploited

### Public Works

Degree to which public utilities (power & water) can be relied upon or must be managed by MARFOR engineers; identification of key nodes to be controlled or protected

### Public Transport

Degree to which civilian transportation assets can be used to support or oppose mid-term MARFOR stability ops (actual infrastructure covered in Operational Geography)

## Natural Resources

### Contiguous Hostile Areas

Establishes whether or not safehaven areas are available for opposing forces, and whether direct overland logistics resupply is possible. Identifies expanded AO.

### Water Supply

Identifies degree to which water supply might constrain MARFOR as well as local elements, and whether engineer support will be needed to assure water for MARFOR and/or civilians

### Food Supply

Identifies degree to which food supply might constrain local elements, and whether engineer support and imported staples will be required for civilians

### Energy Supply

Identifies degree to which energy supply might constrain MARFOR as well as local elements, and whether engineer support will be needed to assure energy for MARFOR and/or civilians

### Strategic Minerals & Raw Materials

Identifies presence or absence of minerals & raw materials critical to production of war supplies as well as national economy

### Production Base

Identifies income-producing areas or lack of alternatives which may constrain long-term stability & undermine internal security

### Land Tenure

Orients MARFOR regarding existing land distribution/exploitation practices which may stimulate long-term hostility in rural area and/or require civilian assistance

# INSURGENCY FACTORS SHAPING THE EXPEDITIONARY ENVIRONMENT

## Executive Summary

- Insurgency factors shaping the expeditionary environment all fall within existing factors under the military and civilian elements of the framework for expeditionary analysis. However, in recognition of their importance, and the efforts of the Army-Air Force Center for Low Intensity Conflict, this section builds on the results of the "Indicators Templating" study, and presents a tailored framework for drawing high-level generalizations about insurgency factors.
- The five matrices extracted from the study and then refined or expanded include:
  - Insurgent Military Capabilities      -- Host Country Military Capabilities
  - Insurgent Civil Factors              -- Host Country Civil Factors
  - Insurgent Event Data
- Examples of a "high", "medium", and "low" environment for these factors is offered below:
  - High:
  - Medium:
  - Low:

INSURGENCY FACTORS SHAPING THE EXPEDITIONARY ENVIRONMENT

INSURGENT MILITARY CAPABILITIES	HOST COUNTRY MILITARY CAPABILITIES	INSURGENT CIVIL FACTORS	HOST COUNTRY CIVIL FACTORS	INSURGENT EVENT DATA
Commitment to Terrorism	Leadership	Overt Political Mobilization	Police Operations	Bombings
Capability for Terrorism	Military Intelligence	Covert Political Mobilization	Civilian Intelligence Operations	Kidnapping & Assassination
Safe-Haven or Controlled Territory	Troop Discipline & Behavior	Propaganda	Civil-Military Relations	Civil Disobedience
Steady Flow of Weapons & Trained G's	Use of Popular Militia	Civil Acquisition	Unified Management	Strikes & Riots
Established Military Organization	Force Structure	Funding Mechanism	Psychological Operations	International Media Events
Acquisition of Crew-Served Wpns & Vehicles	Strategy	Indoctrination Mechanism	Political Environment	Conventional Military Ops
Established C4I2 Networks	Tactics	Admin & Logs Mechanisms	Administrative & Legal Reforms	International Legal Activity



INSURGENT MILITARY CAPABILITIES SHAPING THE EXPEDITIONARY ENVIRONMENT

CAPABILITY	HIGH COMPLEXITY	MEDIUM COMPLEXITY	LOW COMPLEXITY
COMMITMENT TO TERRORISM	Leaders & followers committed to global campaign of terrorism	National program of terrorism against selected targets	Only occasional resort to terrorism as method of ops
CAPABILITY FOR TERRORISM	International support network and freedom of movement	Limited ability to conduct terrorist acts away from home	Limited to local acts of terrorism
SAFE-HAVEN OR CONTROLLED TERRITORY	Multiple controlled areas and/or adjacent countries offering S/H	Mixed rural-urban controlled areas &/or single S/H country	Small rural area or no regular control, free night passage
STEADY FLOW OF WEAPONS & TRAINED G'S	Regular deliveries of arms, established training areas	Occasional shipment of arms, foreign & informal training	Sporadic & limited arms deliveries, no regular training
ESTABLISHED MILITARY ORGANIZATION	National military command & regional command structure	Informal coordination among separate regional mil. ldrs.	Popular leaders of small bands or cells with no staff
ACQUISITION OF CREW-SERVED WEAPNS & VEHICLES	Regular pipeline for introduction of larger wpns & mil. vehicles	Shoulder-held SAMs & heavy MG, mortars, use commercial veh.	Limited to small arms, grenades; walk & use animals
ESTABLISHED C4I2 NETWORKS	National & regional radio & informant networks w/security	Some mobile radio equipment, crude intelligence nets	Limited to personal & commercial comms, personal obsvtn.

# HOST COUNTRY MILITARY CAPABILITIES SHAPING THE EXPEDITIONARY ENVIRONMENT

CAPABILITY	HIGH COMPLEXITY	MEDIUM COMPLEXITY	LOW COMPLEXITY
LEADERSHIP	Opportunistic & corrupt leaders w/o scruples	Trained officers, no/untrained NCOs, conscripted troops	Highly professional, military sensitive to popular concerns
MILITARY INTELLIGENCE	Only informal sources & no standard methods for intel processing	Provincial networks under informal control	Organized networks & data handling techniques
TROOP DISCIPLINE & BEHAVIOR	Conscripted troops of different ethnic or regional origin	Untrained troops inclined to violent repression	Trained disciplined troops sensitive to popular concerns
USE OF POPULAR MILITIA	Marginal militia not integrated into military structure	Organized militia independent of regular military	Organized militia fully integrated into regular struc.
FORCE STRUCTURE	Paramilitary force without counter-insurgency training	Military ground force, limited air, some CI training	Complete combined arms force including SO/CI forces
STRATEGY	Top-level refusal to adopt national civil-military strategy	Limited commitment to partial strategy for CI operations	National political & military commitment to CI strategy
TACTICS	Troop leaders refuse to adopt appropriate tactics (e.g. night)	Some troop leaders experiment with & adopt CI tactics	Full understanding & commitment to CI tactics in military

INSURGENT CIVIL FACTORS SHAPING THE EXPEDITIONARY ENVIRONMENT

CAPABILITY	HIGH COMPLEXITY	MEDIUM COMPLEXITY	LOW COMPLEXITY
OVERT POLITICAL MOBILIZATION	Full range of front organizations & ties, int'l representation	One or more front organisations, some political support	Exist as faction within established pol/labor group
COVERT POLITICAL MOBILIZATION	International covert network for channeling funds & information	National covert network, limited int'l connections	Covert cells in select rural/urban areas
PROPAGANDA	High-profile int'l network able to feed video/print material	Organized media strategy & manning, some production	Staged local events with verbal briefs for media
CIVIL ACQUISITION	Full capability to acquire & distribute equip, clothes, food	One-time or ad hoc procurement of items in bulk	Occasional thefts to obtain specific needed items
FUNDING MECHANISM	Int'l financial net with regular flow of funds from supporters	National protection racket or other stable funding	Occasional thefts or reliance on local contributions
INDOCTRINATION MECHANISM	Established ideology & political/economic program w/training	Populist program w/simplistic goals but no training	No established program or indoctrination
ADMIN & LOGS MECHANISMS	Organized files & property control, accountability	Personal files & oversight, some coordination	Limited or no record keeping & accountability

**HOST COUNTRY CI: ACTORS SHAPING THE EXPEDITIONARY ENVIRONMENT**

<b>CAPABILITY</b>	<b>HIGH COMPLEXITY</b>	<b>MEDIUM COMPLEXITY</b>	<b>LOW COMPLEXITY</b>
<b>POLICE OPERATIONS</b>	Personal or para-military police w/o public peace role	Organized police w/limited ability to ensure peace	Integrated national police force fully committed to peace
<b>CIVILIAN INTELLIGENCE OPERATIONS</b>	Opportunistic, corrupt, or limited civilian intelligence org.	Urban/rural-based civilian intel with personal networks	National integrated civilian intel with sources & methods
<b>CIVIL-MILITARY RELATIONS</b>	Completely autonomous military independent of civilian control	Working relations btw civil authority & military forces	Military fully subordinate & supportive of civil.
<b>UNIFIED MANAGEMENT</b>	Autonomous or dis-organized agencies unable to coord.	Organized military w/police cooperation in some areas	Fully integrated civil-military ops across host country
<b>PSYCHOLOGICAL OPERATIONS</b>	Government unwilling to sponsor PSYOP or lacking in credibility	Limited topic or duration PSYOP if external assist.	Full PSYOP program with quality effort & good media access
<b>POLITICAL ENVIRONMENT</b>	Government does not appeal to populace, lacks legitimacy	Government neutral, military or security forces unpopular	Government and its forces appeal to populace
<b>ADMINISTRATIVE &amp; LEGAL REFORMS</b>	Civil or military refusal to compromise or sponsor reforms	Limited admin & legal reforms w/o full enforcement	Fully enforced reforms w/strong military support

INSURGENT EVENT DATA SHAPING THE EXPEDITIONARY ENVIRONMENT

CAPABILITY	HIGH COMPLEXITY	MEDIUM COMPLEXITY	LOW COMPLEXITY
BOMBINGS	Deliberate & frequent bombings of key infrastructure nodes	Occasional major bombing campaigns throughout country	Random bombings for effect on public & private property
KIDNAPPING & ASSASSINATION	Routine kidnappings for funds & routine assassination of pols.	Occasional kidnapping for effect, selected assassina.	Random kidnappings or assassinations
CIVIL DISOBEDIENCE	Strong labor/school support, large public shows of solidarity	Occasional major demonstrations w/o violence	Infrequent public demonstrations, limited turnouts
STRIKES & RIOTS	Regular strikes & riots paralyzing the economy	Occasional strikes or riots affecting areas or industries	Infrequent strikes or riots limited in scope & duration
INTERNATIONAL MEDIA EVENTS	Daily or weekly events staged for or communicated to int'l media	Monthly int'l media events, or advance notice of ops	Occasional local events of limited interest to media
CONVENTIONAL MILITARY OPS	Established campaign of national scope with artillery support	Regional campaign with good C412, mortars, SAMs	"Hit & Run" tactics only, reliance on escape vice arms
INTERNATIONAL LEGAL ACTIVITIES	Established territory & controlled populace, attempted recognition	Routine appeals to int'l organizations for observer status	No basis for legal recognition, no real attempts

## APPENDIX F-2

### Mission Area Factors Summary


#### A. TERMS OF REFERENCE INTRODUCTION

Mission area factors were developed by the Marine Air-Ground Task Force (MAGTF) Integration Section Proponency and Requirements Branch of the MAGTF Warfighting Center to show the various threats and conditions that may be encountered by warfighters when operating in the countries of the expeditionary environment. The following charts depict the mission area factors and outline the criteria for levels of difficulty (thresholds) within each factor.

#### MISSION AREA FACTORS: THREAT

<u>MISSION AREA</u> <u>FACTORS</u> <u>THREAT</u>	<u>CRITERIA</u> <u>LEVELS OF DIFFICULTY</u>						
Drugs	Low			Medium			High
Terrorism	Low	Medium -			Medium -		High
Gray Arms/Tech Transfer	Low			Medium			High
Consolidated Threat	Negligible	1 of 3			2 of 3		All 3
General Ground OOB							
Infantry	Drat/No TR	Drat/TR	PM/No Exp	PM	Reg/TR		Reg/Exp
Armor	None	M-48/T-54/LAV	M-60, AA	T-62E/MOD 55	T-72M1		T-80/64B
Artillery	None	Mortars	How/SP	>30K Range/ FASCAM/TGM	>30K Range/NBC		BLOC
General Air OOB							
Air OOB	None	DC-3/Props	Day/VFR Jets	Early Radar	3d Gen Radar		BLOC
Close Air	None	Props	Day Jnt Atk	Early Sman	STD-OFF PGM		NT/AW
AAW(IAD)	None	Early AAA	Hand-Held SAMs	EW Radar	3d Gen SAMs		BLOC
General Naval OOB							
Naval OOB	None	Small Surface	DEST/FRIG	ASUW/Air/ASW	FWW Carrier		NT/AW
S/S Miss	None	HE	Multi Warhead	High/Flex	Countermeasures		BLOC
			HE/BC	Trajectories			
Patrol Craft	None	Speed Boats	Sm Gun Boats	Lg Gun Boats	ASUW/Air/Air		BLOC
NBC	None	Chem Weap/ No Delivery	Chem Weap/ With Delivery	Chem Weap/ Used	Chem/Bio Used		Nuc/Chem Avail Conflicts
Ongoing Conflicts	No Conflicts						

#### MISSION AREA FACTORS: ENVIRONMENT

<u>MISSION AREA</u> <u>FACTORS</u> <u>ENVIRONMENT</u>	<u>CRITERIA</u> <u>LEVELS OF DIFFICULTY</u> 					
	Low	Medium			High	
U.S. Equities						
Culture						
Language	English	Spanish/French		Arabic	All Others	
Religion	Christian	Christian Orthodox		Eastern/Tribal/Islam	Islam	
Weather	Dry/Warm	Wet/Warm	Mixed	Dry/Hot	Wet/Hot	Wet/Cold
Gen Geo Cond	Urban	Desert		Jungle		Mountainous
OP Elevation	<2000 Ft	<4000 Ft	<6000 Ft	>6000 Ft	>8000 Ft	>12000 Ft
Cross-Country Mob	Generally Suited		Partially Suited			Generally Unsited
Intervisibility (LOS)	>2000 Meters		1000-2000 Meters			<1000 Meters
Hydrography- NGF	Good	Fair		Poor		Unsatisfactory
Hydrography- Coastal Threat	US NGF Advantage		US NGF and Threat Equal			Threat Advantage

#### MISSION AREA FACTORS: LOGISTICS

MISSION AREA FACTORS LOGISTICS	CRITERIA LEVELS OF DIFFICULTY					
MC&G Coverage	1:30 New	1:30 Old	Some 1:30	MSI Avail	1:30 New	None
Airfields	>1/C-3	1/C-3	>3/C-130	3-4/C-130	1/C-130	None
Ports	Wide Harbor/ >50' Depth	Wide Harbor/ >40' Depth	>40' Depth	25-30' Depth	25-34' Depth	None
Key Installations	None	Few Sites	Multi Sites	Pipeline	Oil Field	NBC
MEU Response Time	<2 Days	>2 - <4 Days		>4 - <6 Days		>6 Days
NEO						
Embassy Staff	<25	<50	<100	<250	<500	>500
Evacuees	None	<100	<200	<300	>300	>500 *
Inland Obj	Coastal	<100 NM	<300 NM	>300 NM	>600 NM	>999 NM

\* For purposes of this study, 500 evacuees was used as a threshold. Anything above 500 would probably require consideration of other options, i.e., evacuation by airlift or sea5th.

\* For purposes of this study, 500 evacuees was used as a threshold. Anything above 500 would probably require consideration of other options, i.e., evacuation by airlift or seaSH.

These mission area factors define the critical conditions, situations, threats, and logistical constraints which, when taken together with the countries identified, show various levels or thresholds of difficulty for conducting military operations. This product represents a totally new approach to intelligence for warfighters because it evaluates and classifies countries in relationship to mission area factors and levels of difficulty assigned by warfighters themselves. The mission area factors do not represent a "fixed" list but constitute a "snapshot" based on their initial development in 1989 and 1990. The way in which thresholds between levels of difficulty for each factor are defined can be expected to change over time. Our intent at this stage has been to inform, to provide a useful reference that does not need to be locked up, and to establish an introductory baseline from which more detailed and precise factors and thresholds of difficulty can be developed.

The following charts provide a consolidated overview of selected mission area factors for those countries which represent the greatest combination of threat, terrain, and logistic challenges to the MAGTF. Such countries would be good candidates as models for the testing of USMC scenarios.

**MISSION AREA FACTORS OVERVIEW - THREAT**

REGION	COUNTRY	DRUGS	TERROR	GRAY ARMS	CNO	AIR	NAV	NSC
WESTERN HEMISPHERE	CUBA	●	●	●	●	●	●	●
	MEXICO	●	●	●	●	●	●	●
MIDDLE EAST, SOUTHWEST ASIA	IRAN	●	●	●	●	●	●	●
	IRAQ	●	●	●	●	●	●	●
	LIBYA	●	●	●	●	●	●	●
	SYRIA	●	●	●	●	●	●	●
AFRICA	SOUTH AFRICA	●	●	●	●	●	●	●
ASIA/PACIFIC	INDIA	●	●	●	●	●	●	●
	INDONESIA	●	●	●	●	●	●	●
	JAPAN	●	●	●	●	●	●	●
	NORTH KOREA	●	●	●	●	●	●	●
	PAKISTAN	●	●	●	●	●	●	●
	PRC	●	●	●	●	●	●	●
	THAILAND	●	●	●	●	●	●	●
	VIETNAM	●	●	●	●	●	●	●
EUROPE MED	GREECE	●	●	●	●	●	●	●
	ITALY	●	●	●	●	●	●	●
	TURKEY	●	●	●	●	●	●	●

↑  
INCREASING INVOLVEMENT

**MISSION AREA FACTORS OVERVIEW - ENVIRONMENT AND LOGISTICS**

REGION	COUNTRY	CULT	WX	TERR	NGF	MC LG	FAC	LIFT	NEO
MIDDLE EAST, SOUTHWEST ASIA	IRAN	●	●	●	●	●	●	●	●
	NORTH YEMEN	●	●	●	●	●	●	●	●
	OMAN	●	●	●	●	●	●	●	●
	SOUTH AFRICA	●	●	●	●	●	●	●	●
AFRICA	MADAGASCAR	●	●	●	●	●	●	●	●
	SOMALIA	●	●	●	●	●	●	●	●
	SUDAN	●	●	●	●	●	●	●	●
	UGANDA	●	●	●	●	●	●	●	●
ASIA/PACIFIC	ZAMBIA	●	●	●	●	●	●	●	●
	AFGHANISTAN	●	●	●	●	●	●	●	●
	BANGLADESH	●	●	●	●	●	●	●	●
	BURMA	●	●	●	●	●	●	●	●
	PAKISTAN	●	●	●	●	●	●	●	●
	PRC	●	●	●	●	●	●	●	●
	THAILAND	●	●	●	●	●	●	●	●

↑  
INCREASING DIFFICULTY

## B. CRITERIA AND SUMMARY ASSESSMENTS

The following pages will address each of the mission area factors separately and further describe the criteria by which levels of difficulty were established. These discussions will also include a summary assessment (taken from Volume I) of how individual factors impact on the 69 countries which presently comprise the expeditionary environment.

## DRUG THREAT

### CRITERIA FOR LEVELS OF DIFFICULTY

#### HIGH:

- Major drug producing and/or processing countries
- Heavy involvement in support functions for drug trafficking.

#### MEDIUM:

- Minor drug producing and/or processing countries
- Primary involvement is in one or more of the following.
  - Money laundering
  - Drug transshipment
  - Supply of precursor chemicals

#### LOW:

- Drugs are of little significance.

Using this criteria, countries were classified into the three threat categories through research of the data sources. These sources included, but were not limited to the following:

- (1) Annual Report of the Organized Crime Drug Enforcement Task Force Program, Fiscal Year 1988
- (2) Defense Science Board Summer Study 1987, Detection and Neutralization of Illegal Drugs and Terrorist Devices, October 1987
- (3) U.S. Department of State, Bureau of International Narcotics Control, Strategy Report, March 1989

### SUMMARY ASSESSMENT OF IMPACT ON EXPEDITIONARY ENVIRONMENT COUNTRIES

The "war on drugs" is developing into a real war and Latin America in particular offers a "target rich" environment where Marine Corps forces can expect to be on call to assist law enforcement agencies.

In Asia, the "Golden Triangle" where Burma, Thailand, and Laos share a border is the center of the heroin trade, and this area should also see an increase in joint military-law enforcement activity in the future.

The top three drug trafficking countries were considered to be Colombia, Peru, and Burma. Overviews of those countries are as follows:

(1) Colombia is the center of South American cocaine trafficking, the world's largest producer of marijuana and the world's third largest producer of coca. This country has destroyed more than 90 percent of the cannabis growing in traditional northern areas, but traffickers have planted extensively in the San Lucas Mountains and south in Cauca. Marijuana tonnage increased in 1988 despite an aggressive eradication campaign. Coca cultivation increased above the 1987 level although eradication of 230 hectares was conducted manually. Despite police efforts to harass the Medellin cartel and other trafficking groups, large amounts of cocaine continued to flow to the U.S.; almost 20 metric tons were seized by U.S. Customs. Overall enforcement remains hampered by a judicial system that has been intimidated by violence. Drug profits flow into and out of Colombia, but money laundering presently is not a major activity.



(2) **Peru** is the world's largest producer of coca with between 97,000 to 124,000 metric tons harvested in 1988. In addition, it converts much of its coca into coca paste and is a primary supplier of this substance to Colombian cocaine refineries. Enforcement in the **Upper Huallaga Valley**, the major growing zone for coca remains quite hazardous.

(3) **Burma** is the world's largest producer of opium with between 1,065 to 1,500 metric tons harvested in 1988. Political turmoil in the country has grounded its large-scale aerial eradication program until an effective Government is seated in **Rangoon**. Traffickers capitalized on diminished enforcement efforts to smuggle large quantities of opium and heroin with little interference. The prospect for the future is grim; with highly favorable climatic conditions and the suspension of programs to destroy crops or seize shipments of drugs or precursor chemicals from **China, Thailand, and India**, traffickers may harvest and move annually as much as 1,400 metric tons of opium to heroin refiners in **Southeast Asia**.

The following matrix shows the expeditionary environment countries that are most involved in drug production and trafficking:

### MOST SIGNIFICANT DRUG COUNTRIES TYPES OF THREAT

	DRUG PRODUCTION	DRUG PROCESSING	PRECURSOR CHEMICALS	MONEY LAUNDERING	TRANSIT POINT
<b>WESTERN HEMISPHERE</b>					
ARGENTINA		X	X	X	X
BOLIVIA	X	X			
BRAZIL	X	X	X		X
COLOMBIA	X	X	X		
ECUADOR	X		X		X
JAMAICA	X				X
MEXICO	X				X
PANAMA			X	X	X
PERU	X	X			
<b>MIDDLE EAST</b>					
IRAN	X				X
<b>ASIA</b>					
AFGHANISTAN	X				
BURMA	X				
LAOS	X				
PAKISTAN	X				
THAILAND	X	X	X		

### PLANNING AND PROGRAMMING IMPLICATIONS

In fighting the "war on drugs", the most common form of military assistance is expected to be wide-area surveillance and interdiction. This challenge will tax to the utmost Marine Corps reconnaissance, intelligence, and communications assets. The nature of the target being sought, generally a single nondescript platform integrated among many legitimate aircraft or ocean-going vessels, will require development of close working relationships and fast-reaction capabilities responsive to civilian intelligence and law enforcement leads. The requirements for liaison to law enforcement agencies could become as demanding, and as frustrating, as the present requirements for liaison to various remote theater staffs; Command and Control, Communications, Computers, Intelligence and Interoperability (C4I2) requirements and capabilities will "Make or Break" Marine Corps forces assigned a role in the war on drugs.

Mission Area Factors - 4

## TERRORISM THREAT

### CRITERIA FOR LEVELS OF DIFFICULTY

**HIGH:** Countries found to have a significant association with terrorism, either through state-sponsored terrorism, organizational terrorism, or insurgent terrorism, or a combination of the three

**MEDIUM TO HIGH:** Countries which have had past association and still maintain a residual involvement in terrorism, but to a lesser degree than high threat countries.

**LOW TO MEDIUM:** Countries largely characterized by internal revolutionary activity and related incidents where terrorism plays a role

**LOW:** Countries with little or no association with terrorism.

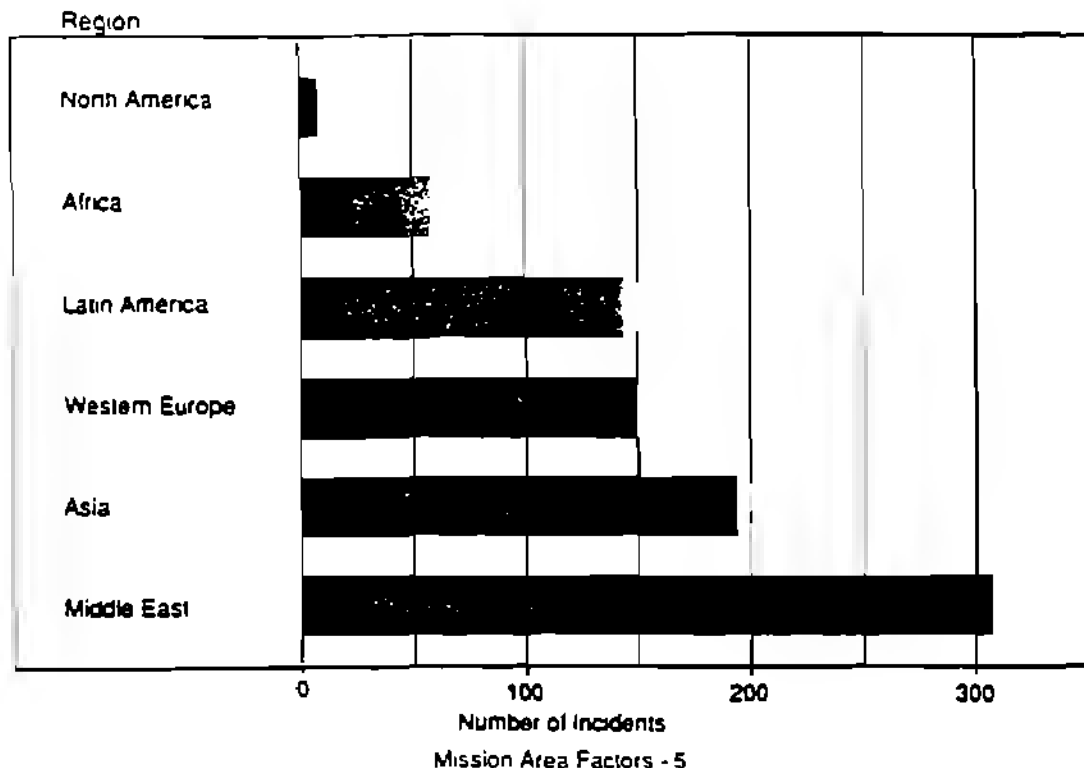
Based on this criteria, countries were classified into the four categories through research of the reference material. This included, but was not limited to the following publications:

- (1) Patterns of Global Terrorism: 1988, Department of State Publication 9705, Office of the Secretary of State Ambassador-at-Large for Counterterrorism, March 1989.
- (2) Terrorist Group Profiles, U.S. Government Printing Office, November 1988.

### SUMMARY ASSESSMENT OF IMPACT ON EXPEDITIONARY ENVIRONMENT COUNTRIES

The level of international terrorist activity worldwide increased by three percent in 1988 with 856 incidents as compared with 832 in 1987. As shown in the following chart, the **Middle East** continued to be the region most affected, incurring 313 attacks or 36 percent of the total worldwide. When **Middle East** spillover attacks are added **Middle East**-inspired terrorist incidents account for 41 percent of the total. **Asia**, primarily due to terrorist attacks by Afghanistan against targets in Pakistan, held second place with 195 incidents or 22 percent of the total.

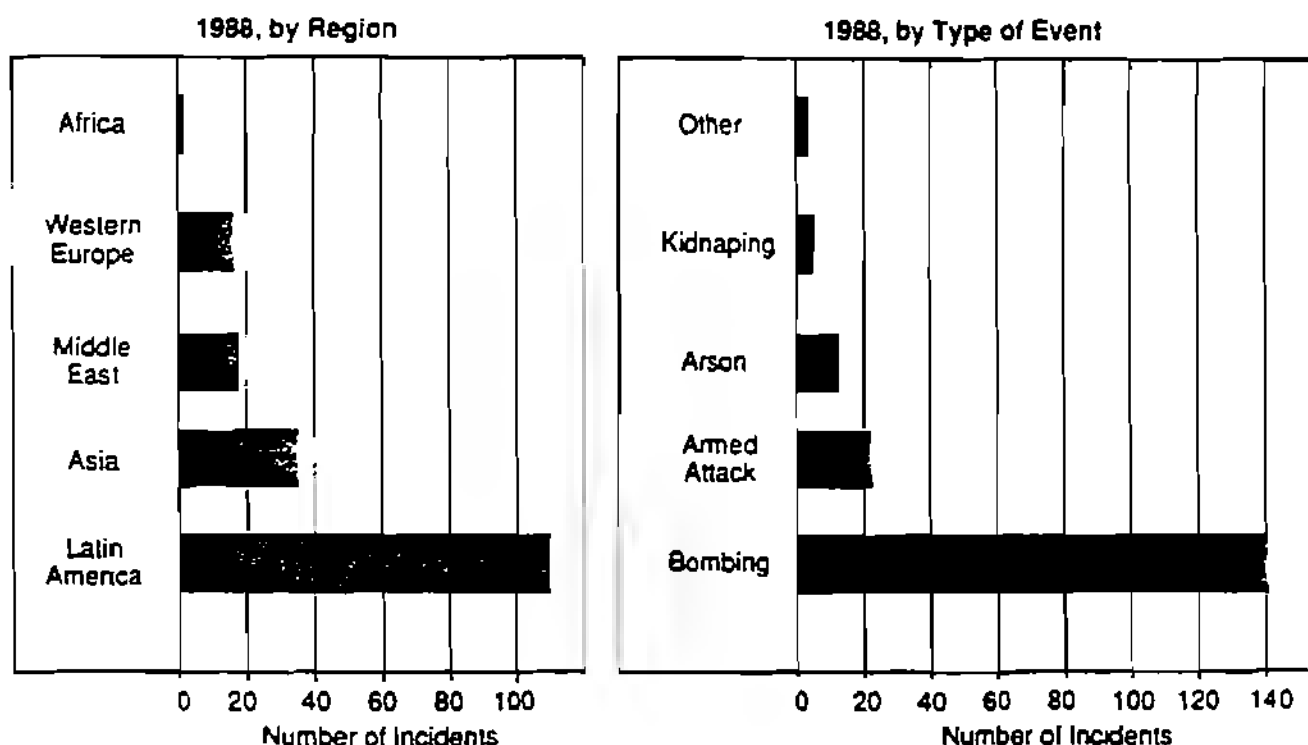
**INTERNATIONAL TERRORIST INCIDENTS, 1988**



As illustrated in the next two charts, the U.S. sustained a substantial number of attacks and casualties abroad in 1988, indicating that it remains a primary target for international terrorists. The number of anti-U.S. incidents increased in all regions, rising from 149 in 1987 to 185 in 1988, and resulting in 192 persons killed and 40 injured. Latin America was the locus of 60 percent of the incidents against U.S. citizens and property. About 20 percent of the anti-U.S. incidents took place in Asia while 10 percent were in the Middle East and 9 percent in Western Europe.

In 1988, 48 percent of the terrorist attacks involved bombings. Armed attacks came next with 29 percent, followed by arson at 15 percent. Terrorists decreased their use of kidnappings as a method in 1988, with only 4 percent of the total. Of the 32 kidnapping incidents worldwide, 12 took place in Latin America. This was a change from 1987 when most of the kidnappings occurred in the Middle East.

## ANTI-U.S. TERRORIST ATTACKS



### PLANNING AND PROGRAMMING IMPLICATIONS

Terrorism is an unpredictable global threat. Latin America is the location of the greatest number of terrorist events, while the Middle East contains the greatest number of terrorist training camps and other targetable facilities. Terrorists do not have rules of engagement, and they generally cannot be detected until after they have struck. MAGTFs must plan for perimeter security measures able to deal with the unexpected. As with drugs, preemptive raids could become more common in the 1990's. Also worth consideration is the possibility of a new method of operation developing between Joint Special Operations Forces (SOFs) and MAGTFs. In concept there is much to be said for the use of SOFs to "find and secure" hostages in place, with MAGTF elements being used to execute a hostile NEO on call. The ability to lift, deliver, and evacuate battalion-sized forces from over-the-horizon and into complex urban environments will be essential for this kind of mission.

## GRAY ARMS AND TECHNOLOGY TRANSFER THREAT

### CRITERIA FOR LEVELS OF DIFFICULTY

**HIGH:** Countries found to be sources of gray market arms and technology sales to unstable and potential hostile Third World buyers

**MEDIUM:** Countries which have acted as transit sites or transshipment points for gray arms and technology sales

**LOW:** Countries with no known association with gray arms and technology transfer.

### DEFINITION:

Sales of military and military-related goods that fall between black market sales and open legitimate transactions comprise the gray market. Such grayness originates in the nature of the item being transferred, or in the character of the transaction, or both. In addition to basic weapons transfers, various products fall into the gray zone when they have both civilian and military applications, and if they are being shipped to countries eligible to receive them for civilian but not military use. Computers are good example, as well as communications equipment, unarmed cargo planes, air traffic control radars, and off-road vehicles. A company that ships such equipment to South Africa or another embargoed country, knowing it is intended for military use is engaged in gray-market arms trafficking.

Based on this methodology, countries were classified into the three categories through a rigorous review of the source data. Reference material included

- (1) World Military Expenditures and Arms Transfers 1988, U.S. Arms Control and Disarmament Agency
- (2) Arms Transfers and the Third World: Trends and Developments, Army-Air Force Center for Low Intensity Conflict, Langley Air Force Base, Virginia, July 1988.
- (3) Stockholm International Peace Research Institute (SIPRI) Yearbook 1989, 1988 and 1987

### SUMMARY ASSESSMENT OF IMPACT ON EXPEDITIONARY ENVIRONMENT COUNTRIES

The accompanying chart depicts the countries associated with gray arms sales and technology transfer. It is interesting to note that almost 60 percent of the source countries listed are in Europe while about 30 percent are in Asia.

Great Britain, France, Italy, and West Germany have proven their technological prowess on the international market. Japan has used high technology in home electronics, computers, and semiconductors to gain its current position as an industry leader. Israel, has a significant emerging technological capability.

Individuals and companies operating in countries such as France, Israel, and Japan serve as either sources of arms for the Third World or as conduits through which China, North Korea, Vietnam, Iran, and Iraq illegally acquire restricted U.S. technology. In turn, these countries, as a routine policy, distribute arms and restricted technology to revolutionary groups and terrorists.

During the period 1981 to 1987, 502 individuals and companies were cited in 156 cases arising from violations of the 1976 Arms Export Control Act. However, it is suspected that many of the less visible brokers, financiers, middlemen, and fixers who specialize in covert arms transactions escaped detection.

## COUNTRIES INVOLVED IN GRAY ARMS AND TECHNOLOGY TRANSFER

<u>SOURCES</u>	<u>TRANSIT POINTS</u>	<u>BUYERS</u>
BELGIUM	BELGIUM	AFGHANISTAN
CHINA	BULGARIA	ALGERIA
FINLAND	CHINA	ANGOLA
FRANCE	CUBA	BANGLADESH
INDIA	CYPRUS	COLOMBIA
ISRAEL	GREECE	CUBA
ITALY	HONG KONG	IRAN
JAPAN	ITALY	IRAQ
NETHERLANDS	MEXICO	KENYA
NORTH KOREA	NETHERLANDS	LIBYA
PANAMA	PANAMA	MALAYSIA
SCOTLAND	PORTUGAL	NICARAGUA
SWEDEN	SINGAPORE	NORTH KOREA
TURKEY	SOUTH AFRICA	SOMALIA
UNITED KINGDOM	SOUTH YEMEN	SOUTH AFRICA
VIETNAM	SYRIA	SOUTH YEMEN
WEST GERMANY		SUDAN
		UGANDA
		VIETNAM

### PLANNING AND PROGRAMMING IMPLICATIONS

The sale of arms and technology to the Third World by more developed nations is of an increasing concern to the U.S. Questionable sales of restricted systems and material to unstable Third World countries are occurring largely through third party transfers. Such transfers often involve at least one Third World transit point. Panama for example, is a major transshipment site for computer technology enroute from the U.S. to Eastern Europe. Included in this threat is the proliferation of nuclear, biological, and chemical weapons and manufacturing capabilities, as well as the marketing of "Blue" (allied) weapons systems which cannot be countered without adverse impact on friendly forces. Many of the industrialized countries of Europe as well as emerging Third World countries are showing growth in arms and technology sales in the international market. While efforts are being made by cooperating countries to prevent illegal or questionable sales, they are frequently unsuccessful. Involved countries may not be aware of impending sales or may disagree with a U.S. view against a sale. Furthermore, U.S. attempts to define and restrict "dual-use" technology are frequently years behind industry development, so that such technologies are usually available during their early production. Finally, some private companies and individuals are willing to violate the laws and sell to any interested party for a profit. Gray arms trafficking and technology theft may require the requirements for the employment of Marine forces to destroy arms factories and storage depots, neutralize known stocks of bio-chemical weapons, or confiscate stolen materials.

## CONSOLIDATED THREAT OVERVIEW

### CRITERIA FOR LEVELS OF DIFFICULTY

The most difficult countries are in the "all 3" category which indicates involvement with drugs, terrorism, and gray arms/technology transfer. Progressively lower levels of difficulty are shown by country involvement in "2 of 3", "1 of 3" or "negligible" association with these threats.

### SUMMARY ASSESSMENT OF IMPACT ON EXPEDITIONARY ENVIRONMENT COUNTRIES

The accompanying matrices show the involvement of expeditionary environment countries in the three threat areas of drugs, terrorism, and gray arms/technology transfers. In the Western Hemisphere, Cuba, Mexico, and Panama were the high-threat countries with involvement in all three areas. Eight other countries, or 50 percent of the countries addressed in this region, were associated with both drugs and terrorism.

In the Middle East/Southwest Asia, Syria was the highest threat country, followed by Iran, Lebanon, South Yemen, Egypt, and Libya.

Africa was the lowest overall threat. Only Angola, Kenya, and South Africa were identified with one threat area.

In Asia, India presented the greatest threat with involvement in all areas, while six other countries were identified with two of three areas and six countries with one of three areas.

In Europe/Mediterranean, Greece and Turkey were both high-threat countries followed by Italy with involvement in terrorism and gray arms/technology transfer.

## CONSOLIDATED THREAT OVERVIEW

	NEGLECTIBLE	1 OF 3	2 OF 3	ALL
WESTERN HEMISPHERE	GRENADA	DOM REP (D)	COLOMBIA (D,T)	CUBA
	SURINAM	HAITI (D)	COSTA RICA (D,T)	MEXICO
		JAMAICA (D)	EL SALVADOR (D,T)	PANAMA
			GUATEMALA (D,T)	
			HONDURAS (D,T)	
			NICARAGUA (D,T)	
			PERU (D,T)	
			VENEZUELA (D,T)	
MIDDLE EAST/ SOUTHWEST ASIA	BAHRAIN	EGYPT (D)	IRAN (D,T)	SYRIA
	IRAQ	LIBYA (T)	LEBANON (D,T)	
	KUWAIT		SOUTH YEMEN (T,G)	
	NORTH YEMEN			
	OMAN			
	QATAR			
	SAUDI ARABIA			
	UAE			

KEY    D Drugs  
          T Terror  
          G Gray Arms/Technology Transfer

Mission Area Factors - 9

## CONSOLIDATED THREAT OVERVIEW

	NEGLIGIBLE	1 OF 3	2 OF 3	ALL
AFRICA	ALGERIA	ANGOLA (T)		
	DJIBOUTI	KENYA (D)		
	ETHIOPIA	SOUTH AFRICA (G)		
	LIBERIA			
	MADAGASCAR			
	NAMIBIA			
	SOMALIA			
	SUDAN			
	TUNISIA			
	UGANDA			
	ZAIRE			
	ZIMBABWE			
ASIA/ PACIFIC	BANGLADESH	BURMA (D)	AFGHANISTAN (D,T)	INDIA
	PAPUA N. G.	INDONESIA (D)	NORTH KOREA (T,G)	
	SOUTH KOREA	JAPAN (T)	PAKISTAN (D,T)	
	S. PACIFIC IS.	MALAYSIA (D)	PHILIPPINES (D,T)	
	SPRATLY IS.	SRI LANKA (T)	PRC (D,G)	
		THAILAND (D)	VIETNAM (T,G)	
EUROPE/ MED	DENMARK		ITALY (T,G)	GREECE
	NORWAY			TURKEY
	YUGOSLAVIA			

KEY: D Drugs  
T Terror  
G Gray Arms/Technology Transfer

### PLANNING AND PROGRAMMING IMPLICATIONS

Drug trafficking, terrorism, and gray arms trade are likely to be national security issues in the next decade. MAGTFs, operating as integral components of the balanced fleet, may have to respond to crisis situations in a variety of ways to protect the national interest. These may range from providing security or peacekeeping forces to conducting retaliatory strikes against threat forces. Marines must continually evaluate the threat as well as their operational concepts, doctrine, force structure, and acquisitions to ensure the maximum preparedness for potential contingency operations. Drugs, terrorism, and gray arms "targets" and scenarios require a different force structure, different organization and equipment, and different concepts and capabilities in C4I2. Force planners must also focus on the unique challenges of Third World environments and logistics requirements where Marine forces must operate without being able to turn on the conventional warfare "pipeline."

## GENERAL GROUND ORDER OF BATTLE

### CRITERIA FOR LEVELS OF DIFFICULTY

	LEVELS OF DIFFICULTY (CAPABILITY)					
	A	B	C	D	E	F
General Ground OOB						
Infantry	Draft/No TR	Draft/TR	PM/No Exp	PM	Reg/TR	Reg/Exp
Armor	None	M-48/T-54/LAV	M-60, AA	T-62/MOD 55	T-72M1	T-80/64B
Artillery	None	Mortars	How/SP	>30 Range/ FASCAM/TGM	>30 Range/NBC	BLOC

The expeditionary environment countries were broken into six approximately equal groups based on an assigned total capability value. The groups ranged from "A" with the least general ground Order of Battle (OOB) capability to "F" with the greatest. The total capability value was obtained by assigning points to the various infantry, armor and artillery capabilities, with the most significant capabilities (e.g., Reg/Exp, T-80/64B, BLOC) receiving the most points. Army size and quality (an assessment of training, leadership, combat experience, and general efficiency) were also factored into the total capability value. Volume II, Study Supporting Material, Section 13, General Ground Order of Battle contains more detailed information on this process including the exact point values assigned and the calculations made for each country. The references used as source material for this assessment are as follows:

- (1) The Military Balance, 1988 - 1989
- (2) Defense and Foreign Affairs Handbook, 1989
- (3) World Armies, Second Edition by John Keegan, 1983

### SUMMARY ASSESSMENT OF IMPACT ON EXPEDITIONARY ENVIRONMENT COUNTRIES

The accompanying matrices show the general ground OOB capabilities for expeditionary environment countries. Most countries in the Western Hemisphere had either small or small-to-medium capabilities. The countries with the most significant resources were Cuba, Nicaragua, Colombia, and Mexico.

In the Middle East/Southwest Asia, the countries which stood out with the largest capabilities were Egypt, Iran, Iraq, Syria, Libya, and Saudi Arabia.

## GENERAL GROUND OOB CAPABILITIES

INCREASING CAPABILITY →						
WESTERN HEMISPHERE	COSTA RICA	DOM. REP	EL SALVADOR	COLOMBIA	CUBA	
	GRENADA	HAITI	GUATEMALA	MEXICO	NICARAGUA	
	HONDURAS	PANAMA	PERU			
	JAMAICA	VENEZUELA				
	SURINAM					
MIDDLE EAST/ SOUTHWEST ASIA	KUWAIT	BAHRAIN	LEBANON	SAUDI ARABIA	LIBYA	EGYPT
		QATAR	NORTH YEMEN			IRAN
			OMAN			IRAQ
			SOUTH YEMEN			SYRIA
			UAE			



The most impressive ground OOB capabilities in Africa were found in the countries of Algeria and Ethiopia followed by Angola, Somalia, South Africa, Sudan and Uganda.

In Asia, the countries of India, North Korea, the Peoples' Republic of China, and Vietnam were identified to have the largest capabilities not only in the region, but in the entire expeditionary environment. They were followed by Pakistan, South Korea, Burma, Indonesia, Japan, and Thailand.

In Europe, Turkey had the largest ground OOB followed by Greece, Italy, and Yugoslavia.

## GENERAL GROUND OOB CAPABILITIES

INCREASING CAPABILITY →						
AFRICA	DJIBOUTI	KENYA	MADAGASCAR	ANGOLA	ALGERIA	
	NAMIBIA	LIBERIA	ZAMBIA	SOMALIA	ETHIOPIA	
		TUNISIA	ZIMBABWE	SOUTH AFRICA		
				SUDAN		
				UGANDA		
ASIA/ PACIFIC	PAPUA N. G.	SRI LANKA		AFGHANISTAN	BURMA	INDIA
	S. PACIFIC IS.			BANGLADESH	INDONESIA	NORTH KOREA
	SPRATLY IS.			MALAYSIA	JAPAN	PAKISTAN
				PHILIPPINES	THAILAND	PRC
						SOUTH KOREA
						VIETNAM
EUROPE/ MED		NORWAY	DENMARK		GREECE	TURKEY
					ITALY	
					YUGOSLAVIA	

## PLANNING AND PROGRAMMING IMPLICATIONS

Besides Soviet proxies with advanced weapons systems, the conventional threat includes Third World countries using non-Soviet systems sold to them by allied or nominally friendly countries, and relatively sophisticated systems developed by Third World regional powers. The non-Soviet systems complicate our electronic warfare planning, signal intelligence, and communications; for in some instances we cannot jam them without jamming ourselves, and because of shared frequency spectrums.

The expeditionary environment is complex and lethal. The MAGTF can expect to meet trained and experienced infantry, modern armor, relatively sophisticated artillery including scatterable mines, as well as smart or stand-off munitions. Some countries have sophisticated surface-to-surface missiles and other advanced coastal defense systems.

An overview assessment of capabilities indicates that a MEU could conduct successful operations in countries with a small ground OOB. Depending on intelligence and threat country force dispositions a MEU could also conduct successful raid-type operations against the larger and stronger countries. Such missions as Noncombatant Evacuation Operations (NEO) and other limited objective operations could be conducted with a reasonable chance of success provided there was adequate preparation and naval support. In deciding how to train, equip, and organize Marine Corps forces our planners must constantly evaluate trade-offs between our own capabilities limited by our forward deployed amphibious character and the small size of our forces afloat, and the fully equipped, trained, and generally well organized forces we might confront.

## GENERAL AIR ORDER OF BATTLE

### CRITERIA FOR LEVELS OF DIFFICULTY

	LEVELS OF DIFFICULTY (CAPABILITY)					
	A	B	C	D	E	F
General Air OOB						
Air OOB	None	DC-3/Props	Day/NFR Jets	Early Radar	3d Gen Radar	BLOC
Close Air	None	Props	Day Jet Air	Early Smart	STD-OFF PGM	NT/AW
AAW (IAD)	None	Early AAA	Hand-Held SAMs	EW Radar	3d Gen SAMs	BLOC

The expeditionary environment countries were divided into six approximately equal groups based on an assigned total capability value. The groups ranged from "A" with the least general air OOB capability to "F" with the greatest. The total capability value was obtained by assigning points to the various air OOB, close air support, and Air Tasking Order (AAW)/Integrated Air Defense (IAD) capabilities, with the most significant capabilities (e.g., BLOC, 3d generation radar, Night Time/All Weather (NT/AW), Stand-Off-Precision Guided Munitions (STD-OFF PGM), 3d generation Surface-to-Air Missiles (SAMs)) receiving the most points. Air Force size and quality (an assessment of training, leadership, combat experience, and general efficiency) were also factored into the total capability value. Volume II, Study Supporting Material, Section 14, General Air Order of Battle contains more detailed information on this process including the exact point values assigned and the calculations made for each country. The references used as source material for this assessment are as follows:

- (1) Defense and Foreign Affairs Handbook, 1989
- (2) Jane's All the World's Aircraft, 1988 - 1989
- (3) Jane's Land Based Air Defense Systems, 1989 - 1990
- (4) Jane's Weapon Systems, 1988 - 1989
- (5) Jane's Weapon Systems, 1987 - 1988

### SUMMARY ASSESSMENT OF IMPACT ON EXPEDITIONARY ENVIRONMENT COUNTRIES

The accompanying matrices depict the general air OOB capabilities for expeditionary environment countries. Most countries in the Western Hemisphere are grouped in the lowest three categories. In this region, the countries with the most significant aviation resources were Cuba, Nicaragua, and Peru.

From a global perspective, Egypt, Iran, Iraq, and Syria stood out with the strongest aviation and air defense assets. Other countries in the Middle East/Southwest Asia with large capabilities were Libya, Saudi Arabia, and South Yemen.

## GENERAL AIR OOB CAPABILITIES

INCREASING CAPABILITIES →						
WESTERN HEMISPHERE	COSTA RICA	DOM REP	COLOMBIA	NICARAGUA	CUBA	
	GRENADA	GUATEMALA	EL SALVADOR	PERU		
	JAMAICA	HAITI	MEXICO			
	PANAMA	HONDURAS	VENEZUELA			
	SURINAM					
MIDDLE EAST/ SOUTHWEST ASIA		BAHRAIN	OMAN	KUWAIT	LIBYA	EGYPT
		LEBANON	QATAR	NORTH YEMEN	SAUDI ARABIA	IRAN
			UAE		SOUTH YEMEN	IRAQ
						SYRIA

In Africa, the most impressive air OOB countries were Algeria, Angola, and South Africa.

The most extensive aviation capabilities in Asia/Pacific were found in the countries of India, Japan, North Korea, and the People's Republic of China. They were followed by Afghanistan, South Korea, and Vietnam.

In Europe/Mediterranean, Italy, Turkey, and Yugoslavia had the strongest air OOB followed by Greece, Norway, and Denmark.

## GENERAL AIR OOB CAPABILITIES

INCREASING CAPABILITIES →						
AFRICA	DJIBOUTI	KENYA	SOMALIA	ETHIOPIA	ALGERIA	
	LIBERIA	UGANDA	SUDAN	MADAGASCAR	ANGOLA	
	NAMIBIA	ZAIRE	TUNISIA	ZIMBABWE	SOUTH AFRICA	
ASIA/ PACIFIC	PAPUA N. G.	BURMA	BANGLADESH	INDONESIA	AFGHANISTAN	INDIA
	S. PACIFIC IS.	SRI LANKA	PHILIPPINES	MALAYSIA	SOUTH KOREA	JAPAN
	SPRATLY IS.			PAKISTAN	VIETNAM	NORTH KOREA
				THAILAND		PRC
EUROPE/ MED				DENMARK	GREECE	ITALY
					NORWAY	TURKEY
						YUGOSLAVIA

## PLANNING AND PROGRAMMING IMPLICATIONS

The expeditionary environment in the air is as complex and lethal as that on the ground. The MAGTF can expect to encounter threat aircraft with some night or all-weather capability, as well as smart or stand-off munitions. Iraq, for example, employs MiG-29 aircraft which are kept operationally ready through the assistance of on-site Soviet advisors. Threat integrated air defense systems may include three dimensional long-range radars able to detect stealthy airborne platforms. In this regard, Libya employs an air defense system known as "SENEZH" which is modeled after Soviet equipment and doctrine. China has a relatively sophisticated network of air defense radars which provides surveillance and control, and an early warning system for the detection of hostile missiles. Threat air defense systems may also employ a variety of advanced and strategically placed SAMs. Syria, for example, has some of the most modern Soviet provided SAMs as well as 50,000 personnel in a separate air defense command.

An examination of aviation and air defense capabilities of expeditionary environment countries indicates that a MEU could expect to conduct successful air operations against most lower capability countries. Depending on a variety of factors, such as the operational condition of threat aircraft and air defense weapons, unit locations, and detection capabilities, a MEU could also conduct operations effectively against many of the stronger countries. Given our critical reliance on vertical lift as a primary means of expeditionary mobility, Marine Corps planners must make more provision for the suppression of air defense, survivability of lift aircraft, and availability of close air support for all MAGTF missions with special emphasis on stability operations and low-intensity conflict requirements.

## GENERAL NAVAL ORDER OF BATTLE

### CRITERIA FOR LEVELS OF DIFFICULTY

	LEVELS OF DIFFICULTY (CAPABILITY)					
	A	B	C	D	E	F
General Naval OOB						
Naval OOB	None	Small Surface	DEST/FRIG	ASUW/Air/ASW	FW Carrier	NT/AW
S/S Miss	None	ME	Muhl Warhead	High/Flex	Countermeasures	BLOC
			ME/BC	Trajectories		
Patrol Craft	None	Speeds Boats	Sm Gun Boats	Lg Gun Boats	ASUW/Antair	BLOC

The expeditionary environment countries were divided into six approximately equal groups based on an assigned total capability value. The groups ranged from "A" with the least general naval OOB capability to "F" with the greatest. The total capability value was obtained by assigning points to the various naval OOB, surface-to-surface missile, and patrol craft capabilities, with the most significant capabilities (e.g., NT/AW, Fixed Wing Carrier, Bloc, Countermeasures, Antisurface Warfare (ASUW)/Antair) receiving the most points. The Navy size and quality (an assessment of training, leadership, combat experience, and general efficiency) were also factored into the total capability value. Volume II, Study Supporting Material, Section 15, General Naval Order of Battle contains more detailed information on this process including the exact point values assigned and the calculations made for each country. The references used as source material for this assessment are as follows:

- (1) Jane's Fighting Ships, 1988 - 1989
- (2) Jane's Weapon Systems, 1987 - 1988
- (3) Defense and Foreign Affairs Handbook 1989
- (4) A Quick and Dirty Guide to War by James Dunnigan and Austin Bay, Updated Edition, dated 1986

### SUMMARY ASSESSMENT OF IMPACT ON EXPEDITIONARY ENVIRONMENT COUNTRIES

The accompanying matrices show the general naval OOB capabilities for expeditionary environment countries. In the Western Hemisphere, Cuba was identified as having the greatest naval capability, followed by Colombia, Mexico, Peru, and Venezuela.

In the Middle East/Southwest Asia, Egypt stood out with the most well-equipped naval force followed by Iran, Iraq, Libya, and Syria.

## GENERAL NAVAL OOB CAPABILITIES

INCREASING CAPABILITIES →						
WESTERN HEMISPHERE	GRENADA	COSTA RICA	DOM REP	COLOMBIA	CUBA	
	SURINAM	GUATEMALA	EL SALVADOR	MEXICO		
		HAITI	NICARAGUA	PERU		
		HONDURAS		VENEZUELA		
		JAMAICA				
		PANAMA				
MIDDLE EAST/ SOUTHWEST ASIA	LEBANON		BAHRAIN	SAUDI ARABIA	IRAN	EGYPT
			KUWAIT	SOUTH YEMEN	IRAQ	
			NORTH YEMEN		LIBYA	
			OMAN		SYRIA	
			QATAR			
			UAE			

In Africa the primary naval forces were found in Algeria, Ethiopia, and South Africa followed by Angola, Kenya, and Somalia.

Both Asia/Pacific and Europe Mediterranean have a high proportion of countries with a strong naval force. In Asia, the countries of India, Indonesia, Japan, North Korea, Pakistan, the People's Republic of China, and South Korea were predominate, while in Europe, Italy, Turkey and Yugoslavia had the most extensive capabilities.

## GENERAL NAVAL OOB CAPABILITIES

INCREASING CAPABILITIES →						
AFRICA	DJIBOUTI	MADAGASCAR	TUNISIA	ANGOLA	ALGERIA	
	LIBERIA	SUDAN		KENYA	ETHIOPIA	
	NAMIBIA	ZAIRE		SOMALIA	SOUTH AFRICA	
	UGANDA					
	ZIMBABWE					
ASIA/ PACIFIC	AFGHANISTAN	PAPUA N. G.	BURMA	MALAYSIA	BANGLADESH	INDIA
	S PACIFIC IS.	SRI LANKA	PHILIPPINES		THAILAND	INDONESIA
	SPRATLY IS				VIETNAM	JAPAN
						NORTH KOREA
						PAKISTAN
						PRC
						SOUTH KOREA
EUROPE/ MED				DENMARK	GREECE	ITALY
				NORWAY		TURKEY
						YUGOSLAVIA

## PLANNING AND PROGRAMMING IMPLICATIONS

The expeditionary environment at sea could present some serious challenges for an Amphibious Task Force (ATF) enroute to, or operating in an objective area. India, for example has two fixed wing aircraft carriers (Ex -U.K.), five destroyers, twenty-one frigates, and six corvettes equipped with Surface-to-Surface Missiles (SSMs), SAMs, guns, torpedos, antisubmarine mortars, countermeasures, and radars. Another example of an expeditionary environment country with a strong naval capability is Italy. It has two light aircraft carriers (one can accommodate VSTOL aircraft and helicopters, and one can handle helicopters only), two cruisers, six destroyers, sixteen frigates, and nineteen corvettes all equipped with modern weapons and supporting systems.

A review of the naval capabilities of expeditionary environment countries indicates that those countries depicted in the three most difficult categories would represent a formidable threat to a MEU-sized ATF. Limited objective operations in these countries should be planned to take greatest advantage of intelligence, naval support, and the element of surprise. Marine Corps planners should also pursue continued close coordination with the Navy to focus on the shortfalls in amphibious lift, shallow-water anti-submarine and mine warfare, over-the-horizon delivery, and the suppression of coastal missiles.

# NUCLEAR, BIOLOGICAL, AND CHEMICAL ORDER OF BATTLE

## CRITERIA FOR LEVELS OF DIFFICULTY

NBC	LEVELS OF DIFFICULTY (CAPABILITY)					
	A	B	C	D	E	F
	None	Chem/Weap/ No Delivery	Chem/Weap/ With Delivery	Chem Weap/ Used	Chem/Bio Used	Nuc/Chem Avail

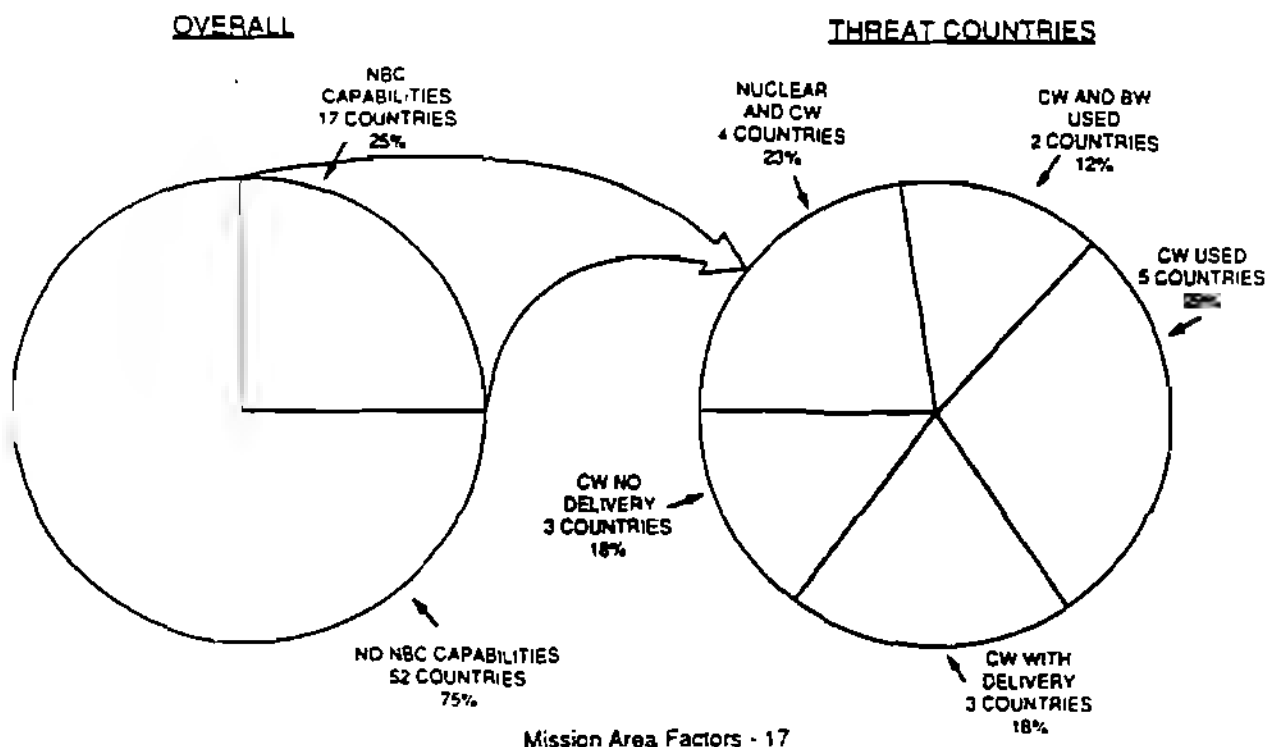
- F** - Countries possessing nuclear and chemical weapons
- E** - Countries which have used chemical and biological weapons
- D** - Countries which have used chemical weapons
- C** - Countries suspected to have chemical weapons with a delivery capability
- B** - Countries suspected to have chemical weapons but without a means of delivery
- A** - Countries believed not to have an NBC weapons capability

Countries in the various categories were identified through a thorough review of open source literature. References most useful to this assessment were the SIPRI Yearbooks, 1989, 1988, and 1987

## SUMMARY ASSESSMENT OF IMPACT ON EXPEDITIONARY ENVIRONMENT COUNTRIES

The accompanying graphics address the expeditionary environment countries which were found to possess varying types and quantities of NBC weapons.

## DISTRIBUTION OF EXPEDITIONARY ENVIRONMENT COUNTRIES BASED ON NBC CAPABILITIES



There were 4 countries, (South Africa, India, Pakistan, and the PRC) thought to possess nuclear and chemical weapons and constitute the greatest threat.

At the next level of threat, there were 2 countries, Iraq and Vietnam, accused of using both chemical and biological weapons.

Next, there were 5 countries reported to have used chemical weapons only. These countries are Cuba, Iran, Libya, Indonesia, and Thailand.

The last two categories of threat were the countries with chemical weapons and delivery means, and those with chemical weapons but without a reported means of delivery. Each of these categories had 3 countries. Egypt, Syria, and North Korea were reported to have chemical weapons with delivery means while Burma, Japan, and South Korea were thought to have only possession.

## NBC THREAT OVERVIEW

	CHEMICAL WEAPONS NO DELIVERY	CHEMICAL WEAPONS WITH DELIVERY	CHEMICAL WEAPONS USED	CHEMICAL WEAPONS AND BIOLOGICAL WEAPONS USED	NUCLEAR AND CHEMICAL WEAPONS
WESTERN HEMISPHERE			CUBA		
MIDDLE EAST/ SOUTHWEST ASIA		EGYPT	IRAN	IRAQ	
		SYRIA	LIBYA		
AFRICA					SOUTH AFRICA
ASIA/PACIFIC	BURMA	NORTH KOREA	INDONESIA	VIETNAM	INDIA
	JAPAN		THAILAND		PAKISTAN
	SOUTH KOREA				PRC

## PLANNING AND PROGRAMMING IMPLICATIONS

The NBC threat must be factored into Service capabilities planning and programming. There are countries, particularly in the Middle East and Asia, that have used bio-chemical weapons and can be expected to use them again. There are increasing numbers of countries that have stocks of bio-chemical weapons, and other countries working to maintain or develop nuclear capabilities. Perhaps most threatening, as NBC technology and weapons proliferate, the opportunities for nongovernmental groups to steal working weapons and active bio-chemical agents increases dramatically. The next decade may well see a large metropolitan area held hostage to the threat of covertly emplaced and remotely detonated bio-chemical or nuclear weapons.

Some MAGTFs, for example those assigned contingency missions in the Middle East and selected countries in Asia, must continue to plan for and stock equipment needed to fight in a contaminated environment. All MAGTFs should be prepared to execute raids to seize and neutralize NBC weapons under development or in transit.

However, it would be imprudent to over-emphasize this threat, which appears in only 25% of the countries of concern to the Marine Corps. One strategy of possible value would be to carefully tailor a single MAGTF and develop MEU (NBC) training and equipping cycles just as we have for MEU (SOC).

## ONGOING CONFLICTS

### CRITERIA FOR LEVELS OF DIFFICULTY

Through a review of the source material, conflicts locations throughout the world were identified. These conflicts fall into five categories: regional conflicts, civil wars, insurgencies, drug related conflicts, and conflicts involving government instability and repression. In many of the situations, various levels of violence and disorder have occurred in the past and threaten to break out again. In other cases fighting occurs continuously or intermittently at the present time. All countries were evaluated for their involvement in conflict situations. Volume II, Study Supporting Material, Section 5, Existing Ongoing Conflicts provides a description of ongoing conflicts in the countries of interest. When research identified conflicts in countries outside the expeditionary environment, they were also described. The following references were used as the principal basis for this assessment:

- (1) Defense and Foreign Affairs Handbook, 1989
- (2) A Quick and Dirty Guide to War, by James F. Dunnigan and Austin Bay, 1986
- (3) The Statesman's Yearbook, 1989 - 1990
- (4) World Almanac and Book of Facts, 1989
- (5) Zones of Conflict: An Atlas of Future Wars, by John Keagan and Andrew Wheatcraft, 1988
- (6) Countries of the World and Their Leaders Yearbook, 1989
- (7) The World in Conflict, by John Laffin, 1989
- (8) Brassey's War Annual 2, A Guide to Contemporary Wars and Conflicts, by John Laffin, 1986

### SUMMARY ASSESSMENT OF IMPACT ON EXPEDITIONARY ENVIRONMENT COUNTRIES

The accompanying chart shows a regional breakdown of conflict locations and the types of conflict involved. In the **Western Hemisphere** there have been various levels of violence and disorder in **El Salvador**, **Guatemala**, **Honduras**, and **Nicaragua** caused by insurgents. Drug related violence, often combined with terrorism and insurgency, is a major problem in **Colombia** and **Peru**.

In the **Middle East**, regional disputes have prevailed in recent years dominated largely, by the **Iran-Iraq War** and **Syrian intervention in Lebanon**. **Syria** would like to take advantage of the civil war in **Lebanon** to expand its borders. The territorial issue between **Israel** and the **Palestinians** is also highly volatile and the possibility of escalated conflict is a major concern. Now, a new confrontation in this region has erupted between **Iraq** and its Arab neighbors, as well as the **U.S.** and most other countries of the world, over the **Iraqi seizure of Kuwait**. Only **Libya**, the **Palestine Liberation Organization (PLO)**, and to a certain degree **Jordan** and **Sudan** seem to side with **Iraq**. This confrontation has potential to be the largest conflict in recent years.

In **Africa**, there are a range of conflicts from the civil wars in **Angola**, **Liberia** and **Mozambique**, to the insurgent violence in **Ethiopia**, to the disorder and bloodshed in **South Africa** over apartheid. In this region, many countries can be characterized by government instability, frequent violence, economic underdevelopment, and acute poverty. The crisis-torn west African country of **Liberia** is an example of an ongoing conflict with poor prospects for resolution in the immediate future. To protect **U.S.** interests, a **MEU** was recently committed in this country to conduct noncombatant evacuation operations and maintain order around the **U.S. Embassy**. In **Ethiopia**, civil war and starvation continue to prevail, while a corrupt and unstable Marxist regime struggles to remain in power. As the **South African Government** continues to support its policy of apartheid and black African groups fight among themselves, there is potential for serious consequences in this country.

In **Asia and the Pacific**, a major share of the 12 conflict countries are involved in insurgencies and/or drug related violence. Countries such as **Afghanistan**, **Cambodia**, and the **Philippines** all have active guerrilla forces trying to overthrow their governments. The "Golden Triangle" where **Burma**, **Thailand**, and **Laos** share a border, is the center of the region's heroin trade as well as frequent clashes between drug traffickers and government authorities. Countries such as **North Korea** have stocks of chemical weapons, and other countries (**PRC**, **India**, and **Pakistan**) are working to expand an already developed arsenal of nuclear weapons. Given the rate at which NBC weapons are proliferating in this region, it is quite likely they will eventually fall into the hands of extremist or terrorist groups.



While Europe and the Mediterranean presently have no active conflicts, there is significant ethnic unrest along with political and economic turmoil in a number of countries that could form the basis for open conflict. Although Poland now has free elections and a non-Communist government, severe economic problems persist and there could be a resurgence of hostility from the people if conditions do not rapidly improve. The longstanding disputes between Greece and Turkey could easily reemerge as they did in 1987. If this should occur over an issue such as the oil rights under the Aegean Sea, it could lead to a war between these two countries which would have serious impact on Europe as well as the U.S.

### CONFLICTS LOCATIONS

WESTERN HEMISPHERE	MIDDLE EAST	AFRICA	ASIA	EUROPE
COLOMBIA (D)	IRAN (R)	ANGOLA (CW)	AFGHANISTAN (I)	POLAND (I/R)
EL SALVADOR (I)	IRAQ (R)	CHAD (R)	BURMA (D)	TURKEY/GREECE (R)
GUATEMALA (I)	ISRAEL (R)	LIBERIA (CW)	CAMBODIA (I)	
GUYANA (R)	LEBANON (CW)	LIBYA (R)	CHINA (R)	
HAITI (I/R)	OMAN (I)	ETHIOPIA (I)	INDONESIA (I)	
HONDURAS (I)	SYRIA (R)	MOZAMBIQUE (CW)	KOREA (N/S) (R)	
NICARAGUA (I)		NAMIBIA (I)	LAOS (D)	
PANAMA (R)		SOUTH AFRICA (I)	MALAYSIA (I)	
PERU (D)		SUDAN (CW)	PAKISTAN (R)	
		WESTERN SAHARA (R)	PHILIPPINES (I)	
		ZAIRE (I/R)	THAILAND (D)	
		ZIMBABWE (I)	S. CHINA SEA (R)	

KEY: R- REGIONAL CW - CIVIL WAR I - INSURGENCY D - DRUGS VR - INSTABILITY/REPRESSION

### PLANNING AND PROGRAMMING IMPLICATIONS

The expeditionary environment is a violent one with numerous existing conflicts and high likelihood of increased instability in the future. The emerging threat of the 1990's is predominantly nongovernmental, nonconventional, dynamic or random, nonlinear, and without rules of engagement or known doctrine. This threat is also difficult to guard against because our national intelligence community does not have an "indications and warnings" capability against these "type" threats, while the emerging enemy, by contrast, has a virtually unlimited source of drug addicts and related criminals that can be mobilized to compromise our own operational security. The emerging threat has added "worst case" scenarios for which MAGTFs must prepare, including the threat of nonconventional attacks, such as bio-chemical attacks against concentrations of U.S. citizens overseas. In view of the diversity of threats it may confront in the future, MAGTFs must train, equip, and organize to be prepared for operations across the spectrum of conflict, while being more thoughtful about what specific roles and missions a single MAGTF can realistically undertake by itself and/or as the vanguard of follow-on forces.

## U.S. EQUITIES OVERSEAS

### CRITERIA FOR LEVELS OF DIFFICULTY

**HIGH** - Countries with substantial U.S. equities.

**MEDIUM** - Countries with moderate U.S. equities.

**LOW** - Countries with few U.S. equities.

For purposes of this assessment, U.S. equities in the countries of interest included:

- Direct investment
- Trade (imports and exports)
- Economic and military aid
- U.S. citizens in residence
- Strategic and tactical equities (e.g., strategic location, U.S. bases, special cooperation)

In the process of determining overall U.S. equities, the following two step methodology was used:

- (1) The monetary values of U.S. direct investment, exports, imports, and U.S. aid for each country were combined and applied to the U.S. \$ Equities scale below. The number of U.S. citizens living in each country was applied to the U.S. Citizen Equity scale:

U.S. \$ EQUITY	
BIL \$S	RATING
>10.00	6
5.00 - 10.00	5
2.50 - 4.99	4
1.00 - 2.49	3
.50 - .99	2
>0 - .49	1
0	0

U.S. CITIZEN EQUITY	
NO. CIT.	RATING
>10,000	6
5,000 - 10,000	5
2,500 - 4,999	4
1,000 - 2,499	3
500 - 999	2
>0 - 499	1
0	0

- (2) The U.S. dollar equity rating and U.S. citizen equity rating were added together and applied to the following overall U.S. equity scale:

OVERALL U.S. EQUITY		
<b>HIGH</b>	-	9-12
<b>MEDIUM</b>	-	5-8
<b>LOW</b>	-	0-4

Volume II, Study Supporting Material, Section 6, U.S. Equities Overseas contains a description of strategic and tactical equities in the respective countries as well as the data for U.S. military and citizen equities on which the ratings were based. The following references were used as source material for this assessment:

- (1) U.S. Department of State, Country Reports on Economic Policy and Trade Practices, 1989
- (2) Defense and Foreign Affairs Handbook, 1989
- (3) Countries of the World and Their Leaders Yearbook 1989, Gale Research, Inc.
- (4) Central Intelligence Agency, The World Factbook, 1988
- (5) U.S. Department of State, Background Notes and Post Reports, 1987 - 1989.
- (6) U.S. Department of Commerce, Statistical Abstract, 1989.
- (7) Consular Affairs Office, U.S. Department of State, Numbers of U.S. Citizens Living in Countries of Interest, 21 - 22 February 1990

### SUMMARY ASSESSMENT OF IMPACT ON EXPEDITIONARY ENVIRONMENT COUNTRIES

The accompanying chart shows a regional distribution of countries by their level of U.S. equity. In the Western Hemisphere, Mexico had the highest ranking with significantly more dollar equity (25.9 billion) and U.S. citizens (322,250) than other countries. It was followed by Venezuela, Panama and Colombia, all with over 5 billion in trade and investment, and over 11,000 U.S. citizens. Overall in this region, just under half the countries (7 of 16) fell into the high category while the remainder were about evenly distributed between medium and low.

Mission Area Factors - 21

In the Middle East/Southwest Asia, Saudi Arabia had by far the largest U.S. equity with over 10 billion in dollar value and 21,600 U.S. citizens. It was followed by Egypt (3 billion dollar equity and 11,210 U.S. citizens). The other countries in this region fell into the low category except for Kuwait and North Yemen which were rated as medium.

In Africa, two thirds of the countries (10 of 15) were rated in the low category. Algeria, Kenya, Liberia, and Zaire were classified medium and only South Africa with 3.5 billion dollar equity and 9,400 U.S. citizens was rated high.

In Asia/Pacific region, Japan surpassed all other countries with almost 122 billion in dollar equity and 41,000 U.S. citizens. The next closest countries in the high rating were South Korea (27 billion dollars and 10,250 U.S. citizens) and the Philippines (6 billion and 120,090 U.S. citizens). Besides the 6 countries in the high category, 4 countries including India and Pakistan were rated medium, and the remainder were low.

In Europe and the Mediterranean, Italy had the highest rating with 25.6 billion in dollar equity and 92,269 U.S. citizens. It was followed by Greece and Norway in the high category. The remaining three countries, Turkey, Denmark and Yugoslavia received a medium classification.

#### U.S. EQUITY OVERSEAS

	LOW	MEDIUM	HIGH
WESTERN HEMISPHERE	CUBA EL SALVADOR GRENADA NICARAGUA SURINAM	GUATEMALA HAITI HONDURAS JAMAICA	COLOMBIA COSTA RICA DOM REP MEXICO PANAMA PERU VENEZUELA
MIDDLE EAST/ SOUTHWEST ASIA	BAHRAIN IRAN IRAQ LEBANON LIBYA OMAN SOUTH YEMEN SYRIA	KUWAIT NORTH YEMEN	EGYPT SAUDI ARABIA UAE
AFRICA	ANGOLA DRIBOUTI ETHIOPIA MADAGASCAR NAMIBIA SOMALIA SUDAN TUNISIA UGANDA ZIMBABWE	ALGERIA KENYA LIBERIA ZAIRE	SOUTH AFRICA
ASIA/PACIFIC	AFGHANISTAN BANGLADESH BURMA NORTH KOREA SOUTH PACIFIC IS SPRATLY IS SRI LANKA VIETNAM	INDIA MALAYSIA PAKISTAN PAPUA NEW GUINEA	INDONESIA JAPAN PHILIPPINES PRC SOUTH KOREA THAILAND
EUROPE/MED		DENMARK TURKEY YUGOSLAVIA	GREECE ITALY NORWAY

#### PLANNING AND PROGRAMMING IMPLICATIONS

With existing conflicts in the expeditionary environment and high likelihood of increased instability in the future, U.S. investments and U.S. citizens no longer enjoy the relative immunity from local violence which characterized earlier decades. The increasing lethality of both Third World governments and nonconventional groups places at risk assets and strategic choke points that in the past could only have been attacked by a major power. The deliberate sinking of a major U.S. vessel in both the Panama Canal and Suez Canal is a threat difficult to defend against. As such threats begin to concern policy-makers, the prospects for the employment of U.S. forces in preemptive attacks will increase. To effectively meet the difficult challenges of the future, Marines must sharpen their abilities for rapid crisis-action planning and be ready to "fight smart" when the time comes to execute a mission.

## CULTURAL FACTORS: LANGUAGE AND RELIGION

### CRITERIA FOR LEVELS OF DIFFICULTY

Cultural Language Religion	LEVELS OF DIFFICULTY			
	A	B	C	D
	English Christian	Spanish/French Christian Orthodox	Arabic Eastern/Tribal/Islam	All Others Islam

**D** - Countries with hard languages other than those specified below combined with the religion of Islam.

**C** - Countries with the Arabic language combined with Eastern, Tribal, or Islamic religions

**B** - Countries with Spanish, French, and other predominately European languages combined with the Christian Orthodox religion

**A** - Countries with the English language combined with the Christian religion

**Note** - In cases where a country did not match a precise level as specified above, an intermediary level between the language and religion was selected, e.g. Liberia with the English language and traditional religion was rated B.

Volume II, Study Supporting Material, Section 17, Cultural Factors: Language and Religion provides tables showing a cultural factors assessment for each country as well as a listing of religions and primary and secondary languages. The references used as source material for this assessment are as follows:

- (1) Special Assistant, USMC Intelligence Center letter 3811 IN 05 of 26 October 1989, Marine Corps Expeditionary Environment Language Requirements
- (2) Countries of the World, 1989, Gale Research Inc.,
- (3) World Almanac and Book of Facts, 1989, Published by Pharos Books, a Scripps Howard Company

### SUMMARY ASSESSMENT OF IMPACT ON EXPEDITIONARY ENVIRONMENT COUNTRIES

The accompanying charts depict the distribution of 69 expeditionary environment countries by culture: language and religion. Almost 60 percent of the countries fall into the two most difficult cultural categories (C and D).

The regions with the hardest languages and the most distant religions were the Middle East/Southwest Asia (Iran most difficult), Africa (Ethiopia and Somalia most difficult), and Asia/Pacific (Afghanistan, Bangladesh, Indonesia, and Pakistan most difficult). The Western Hemisphere and Europe/Mediterranean (with the exception of Turkey and Yugoslavia) were found to have a much closer language and religion association with the U.S

#### CULTURAL FACTORS: LANGUAGE AND RELIGION

FACTORS	A	B	C	D
LANGUAGE	ENGLISH	SPANISH/FRENCH*	ARABIC	ALL OTHERS
RELIGION	CHRISTIAN	CHRISTIAN ORTHODOX	EASTERN/ TRIBAL/ISLAM	ISLAM
NUMBER OF EXPEDITIONARY ENVIRONMENT COUNTRIES	6	22	33	7

\* ALSO INCLUDES GREEK, ITALIAN, DUTCH, PORTUGUESE, DANISH, NORWEGIAN, AND TURKISH

# CULTURAL FACTORS: LANGUAGE AND RELIGION

	A	B	C	D
WESTERN HEMISPHERE	GRENADE JAMAICA	COLOMBIA COSTA RICA CUBA DOMINICAN REPUBLIC EL SALVADOR GUATEMALA HAITI HONDURAS MEXICO NICARAGUA PANAMA PERU SURINAM VENEZUELA		
MIDDLE EAST/ SOUTHWEST ASIA			BAHRAIN EGYPT IRAQ KUWAIT LEBANON LIBYA NORTH YEMEN OMAN QATAR SAUDI ARABIA SOUTH YEMEN SYRIA UAE	IRAN
AFRICA	SOUTH AFRICA UGANDA	ANGOLA LIBERIA ZAIRE ZIMBABWE	ALGERIA DJIBOUTI KENYA MADAGASCAR NAMIBIA SUDAN TUNISIA	ETHIOPIA SOMALIA
ASIAN/PACIFIC	PAPUA NEW GUINEA SOUTH PACIFIC ISLANDS		BURMA CHINA INDIA JAPAN MALAYSIA NORTH KOREA PHILIPPINES SOUTH KOREA SRI LANKA THAILAND VIETNAM	AFGHANISTAN BANGLADESH INDONESIA PAKISTAN
EUROPE/MED		DENMARK GREECE ITALY NORWAY	TURKEY YUGOSLAVIA	

## PLANNING AND PROGRAMMING IMPLICATIONS

Language and religion are two major elements of the "cultural" terrain within which the MAGTFs must conduct stability operations and limited objective operations. Both require intense interaction with the civilian populace during the operation. The good news is that a MAGTF with strong Spanish and French language skills can operate in 79% of the countries studied, as English, Spanish, or French are established as second languages. Arabic, however, remains a weak point, and is required in fully 30% of the countries of concern. Along with Arabic, an understanding of Islam is critical in 36% of the countries.

Intelligence specialists are not the only ones who need language skills. Low intensity operations require many more Marines in occupational specialties as wide-ranging as military police, engineers, and public affairs to be in language designated billets.

The lack of an active duty PSYOP and Civil Affairs capability may pose a dilemma to MAGTFs needing no-notice support but lacking the authority to mobilize reservists. Religion is an important environmental feature. One product that could be developed by the reserves for contingency use would be a series of distinct Codes of Conduct corresponding to each major religion and related ethnic or racial group likely to be encountered by the MAGTF. Such a series should be no more than one page in length per category, and suitable for issuance to the individual Marine.

## CRITICAL WEATHER FACTORS

### CRITERIA FOR LEVELS OF DIFFICULTY

Weather	LEVELS OF DIFFICULTY					
	A	B	C	D	E	F
	Dry/Warm	Wet/Warm	Mixed	Dry/Hot	Wet/Hot	Wet/Cold

- F** - • Precipitation of 70 inches or more annually  
• Temperature of 40 degrees Fahrenheit or below for extended periods
- E** - • Precipitation of 70 inches or more annually  
• Heat index (combined relative humidity and air temperature) of 80 or above for extended periods
- D** - • Precipitation of 12 inches or less annually  
• Heat index of 80 or above for extended periods
- C** - • Precipitation between 12 and 70 inches annually  
• Wide variations in temperature and rainfall throughout a country
- B** - • Precipitation of 70 inches or more annually  
• Temperatures ranging between 40 degrees Fahrenheit and a heat index of 80
- A** - • Precipitation of 12 inches or less annually  
• Temperatures ranging between 40 degrees Fahrenheit and a heat index of 80

Volume II, Study Supporting Material, Section 18, Critical Weather Factors provides tables which show average temperatures, average relative humidity, and average rainfall by country, as well as a rating of overall weather conditions for each country. The references used as source material for this assessment are as follows:

- (1) The Weather Almanac, Gale Research Company, 1981
- (2) The Weather Handbook, A Summary of Weather Statistics for Selected Cities Throughout the United States and Around the World, Conway Research, Inc., 1974
- (3) The New Book of World Rankings, Facts on File, Inc., 1984
- (4) World Facts and Figures, John Wiley and Sons, 1989
- (5) Worldmark Encyclopedia of Nations, 1984
- (6) World Climate Data, Climatic Data Press, 1972

### SUMMARY ASSESSMENT OF IMPACT ON EXPEDITIONARY ENVIRONMENT COUNTRIES

The accompanying chart shows the weather conditions associated with the various regions of the world. For operations in Latin America and the Caribbean, military forces should be prepared for wet and hot conditions, while in the Middle East and Southwest Asia dry and hot conditions prevail.

Africa presents a variety of conditions including some of the most challenging. Asia and the Pacific are primarily wet and hot or to a lesser extent mixed, while Europe has the most difficult conditions in Norway, followed by mixed or variable situations elsewhere.

Within the expeditionary environment, only one country, Norway, had wet and cold conditions which are the most difficult to operate in. There were 33%, or 23 of 69 countries with the next most difficult conditions, wet and hot. Countries such as Colombia, Panama, Liberia, and the Philippines fall within this category.

The next level of difficulty is dry and hot conditions with 24%, or 16 of 69 countries in the expeditionary environment. Countries such as Libya and Angola are in this grouping. This is followed by countries with mixed or highly variable conditions. Here there are 33% of the total, or 23 countries, including Cuba and Iran.

The last two types of weather conditions representing the least operational difficulty are wet/warm with 1% and dry/warm with 8%. Examples of countries with these conditions are Syria and South Africa.

Mission Area Factors - 25

### CRITICAL WEATHER FACTORS

	DRY/WARM	WET/WARM	MIXED	DRY/HOT	WET/HOT	WET/COLD
WESTERN HEMISPHERE	PERU		CUBA DOM. REP. GUATEMALA HAITI MEXICO VENEZUELA		COLOMBIA COSTA RICA EL SALVADOR GRENADA HONDURAS JAMAICA NICARAGUA PANAMA SURINAM	
MIDDLE EAST/ SOUTHWEST ASIA	IRAN SYRIA		LEBANON	BAHRAIN EGYPT IRAQ KUWAIT LIBYA NORTH YEMEN OMAN QATAR SAUDI ARABIA SOUTH YEMEN UAE		
AFRICA	NAMIBIA SOUTH AFRICA		ALGERIA ETHIOPIA KENYA TUNISIA UGANDA ZIMBABWE	ANGOLA DJIBOUTI SOMALIA SUDAN	LIBERIA MADAGASCAR ZAIRE	
ASIA/ PACIFIC		JAPAN	AFGHANISTAN INDIA NORTH KOREA PRC SOUTH KOREA	PAKISTAN	BANGLADESH BURMA INDONESIA MALAYSIA PAPUA N. G. PHILIPPINES S. PACIFIC IS. SPRATLY IS. SRI LANKA THAILAND VIETNAM	
EUROPE/ MED			DENMARK GREECE ITALY TURKEY YUGOSLAVIA			NORWAY

### PLANNING AND PROGRAMMING IMPLICATIONS

As indicated by the above figures, the weather in the expeditionary environment is uniformly hot. This suggests that evaluation standards for vertical lift and other systems should be based on "hot" as the norm rather than as the "extreme" condition. **Norway**, and its cold weather conditions is unique among the countries. The cost to the Marine Corps' and its MAGTFs in maintaining a cold weather capability for this single contingency may merit review.

## GENERAL GEOGRAPHIC CONDITIONS

### CRITERIA FOR LEVELS OF DIFFICULTY

Gen Geographic Conditions	LEVELS OF DIFFICULTY			
	Urban	Desert	Jungle	Mountainous

The most difficult geographic conditions were mountains, followed by jungle, desert, and urban centers. The predominate condition in each country was determined through a review of the reference material. A country was classified as "urban" if 70 percent or more of its population were living in urban areas. References used for this assessment included:

- (1) Countries of the World and Their Leaders Yearbook, 1989, Gale Research Inc.
- (2) The World Almanac and Book of Facts, 1989, Published by Pharos Books, a Scripps Howard Company
- (3) The World Factbook, 1988, Directorate of Intelligence, Central Intelligence Agency

### SUMMARY ASSESSMENT OF IMPACT ON EXPEDITIONARY ENVIRONMENT COUNTRIES

The accompanying charts show a breakdown of country general geographic conditions by regional distribution. In the Western Hemisphere, over half the countries have primarily mountainous conditions. Countries such as Colombia, El Salvador, and Panama fall into this most difficult category. Three countries in the region, Costa Rica, Nicaragua, and Surinam, have predominately jungle conditions which are the next most difficult after mountains.

In the Middle East/Southwest Asia, almost 60 percent of the countries have desert conditions. These include Egypt, Kuwait, and Saudi Arabia. In this region, Iran, North Yemen, and Oman can be characterized as mountainous. Bahrain, Iraq, and Lebanon have 70 percent or more of their populations living in urban centers.

### GENERAL GEOGRAPHIC CONDITIONS REGIONAL DISTRIBUTION

	URBAN	DESERT	JUNGLE	MOUNTAINOUS
WESTERN HEMISPHERE	CUBA		COSTA RICA	COLOMBIA
	MEXICO		NICARAGUA	DOM. REP.
	PERU		SURINAM	EL SALVADOR
	VENEZUELA			GRENADA
				GUATEMALA
				HAITI
				HONDURAS
				JAMAICA
				PANAMA
MIDDLE EAST/ SOUTHWEST ASIA	BAHRAIN	EGYPT		IRAN
	IRAQ	KUWAIT		NORTH YEMEN
	LEBANON	LIBYA		OMAN
		QATAR		
		SAUDI ARABIA		
		SOUTH YEMEN		
		SYRIA		
		UAE		

Mission Area Factors - 27



Africa was found to have a range of conditions. Eight countries such as Algeria, Somalia, and Tunisia have desert conditions, three have jungle (Liberia, Uganda, and Zaire), and four have mountains (Ethiopia, Madagascar, South Africa, and Zimbabwe) as their primary features.

In Asia/Pacific, just under half the countries had mainly jungle conditions. Representative countries in this category were Burma, Indonesia, and Malaysia. Mountainous conditions prevailed in almost 40 percent of the countries in this region. Countries such as Afghanistan, North Korea, South Korea, and the People's Republic of China were in this category.

In Europe/Mediterranean, Greece, Norway, Turkey, and Yugoslavia presented mountainous conditions while Denmark and Italy had mainly urban populations.

## GENERAL GEOGRAPHIC CONDITIONS REGIONAL DISTRIBUTION

	URBAN	DESERT	JUNGLE	MOUNTAINOUS
AFRICA		ALGERIA	LIBERIA	ETHIOPIA
		ANGOLA	UGANDA	MADAGASCAR
		DJIBOUTI	ZAIRE	SOUTH AFRICA
		KENYA		ZIMBABWE
		NAMIBIA		
		SOMALIA		
		SUDAN		
		TUNISIA		
ASIA/ PACIFIC	INDIA	PAKISTAN	BANGLADESH	AFGHANISTAN
	JAPAN		BURMA	NORTH KOREA
			INDONESIA	PAPUA N. G.
			MALAYSIA	PHILIPPINES
			SPRATLY IS	PRC
			SRI LANKA	SOUTH KOREA
			THAILAND	S. PACIFIC IS
			VIETNAM	
EUROPE/ MED	DENMARK			GREECE
	ITALY			NORWAY
				TURKEY
				YUGOSLAVIA

## PLANNING AND PROGRAMMING IMPLICATIONS

The four types of terrain appear with sufficient frequency to require the development of full combined arms capabilities for each: mountains, jungles, deserts, and urban environments. Scenarios corresponding to each of these different environments would be helpful in developing Required Operational Capabilities (ROC)

## OPERATIONAL ELEVATION

### CRITERIA FOR LEVELS OF DIFFICULTY

	LEVELS OF DIFFICULTY					
	A	B	C	D	E	F
OP Elevation	<2000 Ft	<4000 Ft	<6000 Ft	>6000 Ft	>9000 Ft	>12,000 Ft

**F** - Elevations greater than 12,000 feet

**E** - Elevations from 9,001 feet to 12,000 feet

**D** - Elevations from 6,001 feet to 9,000 feet

**C** - Elevations from 4,000 feet to 6,000 feet

**B** - Elevations from 2,000 feet to 3,999 feet

**A** - Elevations from sea level to 1,999 feet

NOTE: In the process of grading each expeditionary environment country, averages were taken of elevations adjacent to coastal areas, capital cities, key installations, important lines of communications, and other areas where Marines would be likely to operate. Data was obtained from reference material, including atlases, encyclopedias, and almanacs.

### SUMMARY ASSESSMENT OF IMPACT ON EXPEDITIONARY ENVIRONMENT COUNTRIES

The accompanying matrices show the regional distribution of countries by operational elevation. In the Western Hemisphere, half the countries had operational elevations between 2,000 and 4,000 feet. The mountainous country of Peru was found to have the highest elevations.

In the Middle East/Southwest Asia, almost 80 percent of the countries were grouped in the elevation categories of less than 4,000 feet and less than 2,000 feet. North Yemen, Iran, and Saudi Arabia had the highest elevations

### REGIONAL DISTRIBUTION OF COUNTRIES BY OPERATIONAL ELEVATION

		< 2,000 FT	< 4,000 FT	< 6,000 FT	> 6,000 FT	> 9,000 FT	> 12,000 FT
WESTERN HEMISPHERE	CUBA	COSTA RICA	GUATEMALA	COLOMBIA	PERU		
	GRENADA	DOM. REP	NICARAGUA	MEXICO			
	SURINAM	EL SALVADOR					
		HAITI					
		HONDURAS					
		JAMAICA					
		PANAMA					
		VENEZUELA					
MIDDLE EAST/ SOUTHWEST ASIA	BAHRAIN	IRAQ	IRAN	NORTH YEMEN			
	EGYPT	LEBANON	SAUDI ARABIA				
	KUWAIT	OMAN					
	LIBYA	SOUTH YEMEN					
	QATAR	SYRIA					
	UAE						

Mission Area Factors - 29

In Africa, the operational elevations ranged between 2,000 and 9,000 feet for all countries

Operational elevations in the countries of Asia/Pacific ranged across most of the categories with Papua New Guinea presenting the most difficult conditions.

In Europe/Mediterranean, Denmark had the lowest elevations while Greece, Norway, Turkey, and Yugoslavia had the highest.

## REGIONAL DISTRIBUTION OF COUNTRIES BY OPERATIONAL ELEVATION

	< 2,000 FT	< 4,000 FT	< 6,000 FT	> 6,000 FT	> 9,000 FT	> 12,000 FT
AFRICA		LIBERIA	ALGERIA	ANGOLA		
		NAMIBIA	DJIBOUTI	ETHIOPIA		
		TUNISIA	SOMALIA	KENYA		
		ZAIRE	SOUTH AFRICA	MADAGASCAR		
			SUDAN			
			UGANDA			
			ZIMBABWE			
ASIA/ PACIFIC	BANGLADESH	INDIA	JAPAN	AFGHANISTAN	PAPUA N. G.	
	BURMA	INDONESIA	PAKISTAN	MALAYSIA		
	SPRATLY IS.	PRC	PHILIPPINES	NORTH KOREA		
	SRI LANKA	S. PACIFIC IS.	SOUTH KOREA			
	THAILAND					
	VIETNAM					
EUROPE/ MED	DENMARK		ITALY	GREECE		
				NORWAY		
				TURKEY		
				YUGOSLAVIA		

The two expeditionary environment countries with the highest elevations are described as follows.

(1) Papua New Guinea contains a complex system of mountains extending from the eastern end of the main island to the western boundary with Indonesia. Precipitous slopes, knife-sharp ridges, great outcroppings of mountains to heights of almost 15,000 feet, and broad upland valleys at altitudes of 5,000 to 10,000 feet characterize this area.

(2) In Peru, the Andes Mountains occupy nearly 27 percent of the land area and represent a formidable natural barrier to transportation and communications between the coast and the interior. The highest mountain, Huascaran, is 22,071 feet above sea level.

### PLANNING AND PROGRAMMING IMPLICATIONS

In preparing for all types of conflict situations, the elevations where Marines will be operating should be a foremost consideration. Particularly in helicopter operations, weather conditions, as well as elevation, must be carefully assessed. The vertical lift of Marines, together with their equipment and supplies, over varied terrain to inland locations is a fundamental requirement for most operations and must receive the careful attention of planners in order to be successfully executed.

## CROSS - COUNTRY MOBILITY

### CRITERIA FOR LEVELS OF DIFFICULTY

		LEVELS OF DIFFICULTY		
		A	B	C
Cross-Country Mobility		Generally Suited	Partially Suited	Generally Unsited

**C** - Large portions of a country are unsuitable for cross-country movement of tracked vehicles due to broken terrain, extensive ground cover, marshes, swamps, and/or significant bodies of water. In those countries where the coastal region prevents tracked movement from the beach to the interior, the entire country is categorized as unsited for tracked movement.

**B** - Significant parts of a country are suitable for cross-country movement of tracked vehicles. For example, the Central Luzon plain of the Philippines is trafficable, while most other parts of the country are mountainous and unsited for tracked movement.

**A** - Large parts of a country can accommodate the cross-country movement of tracked vehicles. Algeria, for example, is primarily desert and suitable for both wheeled and tracked cross-country movement.

**Note:** Trafficability in this assessment reflects the suitability for cross-country tracked vehicle movement. The factor did not address lines of communications, and existing road, rail, and canal networks. The emphasis was on true cross-country movement.

The analytical judgments in this assessment are based on a review of each country's National Intelligence Survey or its follow-on Army Country Profile and were developed by the USMC Intelligence Center staff.

### SUMMARY ASSESSMENT OF IMPACT ON EXPEDITIONARY ENVIRONMENT COUNTRIES

The accompanying charts illustrate the regional distribution of expeditionary environment countries by suitability for cross-country mobility. Over 60 percent of the countries are generally unsited for this movement and an additional 20 percent are only partially suited.

In the Western Hemisphere, almost 80 percent of the countries were found to be generally unsited for cross-country movement by tracked vehicles. Countries such as Colombia, El Salvador, Guatemala, and Peru have extensive mountain ranges while Costa Rica, Nicaragua and Surinam have dense tropical forests that preclude vehicular movement. Only in Cuba, Mexico, and Venezuela, and to a lesser extent Grenada can movement be generally accommodated.

#### GENERAL TRAFFICABILITY/CROSS-COUNTRY MOBILITY

	GENERALLY SUITED	PARTIALLY SUITED	GENERALLY UNSUITED
WESTERN HEMISPHERE	CUBA MEXICO VENEZUELA	GRENADA	COLOMBIA COSTA RICA DOMINICAN REPUBLIC EL SALVADOR GUATEMALA HATI HONDURAS JAMAICA NICARAGUA PANAMA PERU SURINAM

In the Middle East/Southwest Asia, over 40 percent of the countries are generally unsuited for tracked movement. Iran, for example, has rugged hills and mountains, and smaller areas of wetlands covering about two-thirds of its area. However, about 60 percent of this region is generally, or at least partially, suited for movement by tracked vehicles. Egypt and Libya in particular have desert plains which facilitate movement.

Africa was the region with the most countries which could readily accommodate tracked vehicles. Exactly 40 percent of the countries, including Algeria, Ethiopia, and Somalia, were generally suited for tracked movement while an additional 13 percent (Madagascar and Uganda) were partially suited. The remaining 47 percent of the countries, including Angola, South Africa, and Sudan, were generally unsuited due to conditions ranging from forest areas to coastal mountains.

In the Asia/Pacific region trafficability presents a serious problem with 13 of 18 countries or 72 percent generally unsuited for tracked movement. The primary impediments to trafficability are dense tropical jungles, numerous wetlands such as swamps and marshes, and periodic heavy rainfall. Only India was generally suited and Afghanistan, Pakistan, the Philippines, and South Korea partially suited for tracked movement in this region.

Of the six European/Mediterranean countries considered, four were generally unsuited and two were partially suited for tracked movement. The significant mountain ranges in countries such as Greece, Turkey, and Yugoslavia were a principal limiting factor in this region.

#### GENERAL TRAFFICABILITY/CROSS-COUNTRY MOBILITY

	GENERALLY SUITED	PARTIALLY SUITED	GENERALLY UNSUITED
MIDDLE EAST/ SOUTHWEST ASIA	EGYPT LIBYA	BAHRAIN KUWAIT LEBANON QATAR SYRIA UAE	IRAN IRAQ NORTH YEMEN OMAN SAUDI ARABIA SOUTH YEMEN
AFRICA	ALGERIA DJIBOUTI ETHIOPIA KENYA SOMALIA TUNISIA	MADAGASCAR UGANDA	ANGOLA LIBERIA NAMIBIA SOUTH AFRICA SUDAN ZAIRE ZIMBABWE
ASIA/PACIFIC	INDIA	AFGHANISTAN PAKISTAN PHILIPPINES SOUTH KOREA	BANGLADESH BURMA INDONESIA JAPAN MALAYSIA NORTH KOREA PAPUA NEW GUINEA PRC SOUTH PACIFIC IS SPRATLY IS SRI LANKA THAILAND VIETNAM
EUROPE/MED		ITALY TURKEY	DENMARK GREECE NORWAY YUGOSLAVIA

#### PLANNING AND PROGRAMMING IMPLICATIONS

Marine Corps capabilities which are totally dependent on vehicular transport may need to be reevaluated. It merits comment that a premise which led to these generalizations was that if the coastal region of a country was unsuited, the entire country was assumed to be unsuited because heavy vehicles could not get from their offshore launch point to inland objectives. Maritime Prepositioning Ships (MPS) and strategic airlift deployment alternatives were not considered.

## INTERVISIBILITY: AVERAGE LINE OF SIGHT DISTANCE

### CRITERIA FOR LEVELS OF DIFFICULTY

	LEVELS OF DIFFICULTY		
	OPTIMUM	RESTRICTED	POOR
Intervisibility (Line Of Sight)	>2,000 Meters	1,000 - 2,000 Meters	≤1,000 Meters

**POOR** - Average Line Of Sight (LOS) distance is less than 1,000 meters

**RESTRICTED** - Average LOS distance is between 1,000 and 2,000 meters

**OPTIMUM** - Average LOS distance is between 2,000 and 3,000 meters.

Intervisibility is defined as the LOS distance that direct-fire weapons (armor and antiarmor) of the ground combat element can fire without restrictions to visibility and weapons effectiveness in each of the expeditionary environment countries. The firepower of armor and antiarmor weapons is highly dependent on the terrain. Long-range, flat-trajectory weapons cannot effectively utilize their range in cities, forests, industrial areas, and mountainous regions. In covered and broken terrain, armored forces can employ only a fraction of their firepower and light infantry forces have the advantage. Darkness, poor weather conditions, and obscurants on the battlefield will also have a limiting effect on long-range, direct-fire weapons. The more open the terrain and visibility becomes, the better these weapons can realize their full potential.

After a close examination of the source material in relation to the above criteria, each of the expeditionary environment countries was rated according to its intervisibility. Volume II, Study Supporting Material, Section 22, Intervisibility: Average Line of Sight Distance contains an assessment of the conditions within each country on which the ratings were based. The references used as source material for the assessment are as follows:

- (1) Battlefield Central Europe. Danger of Overreliance on Technology by the Armed Forces. Brigadier General Franz Uhle-Wattler, undated.
- (2) Zones of Conflict: An Atlas of Future Wars. John Keegan and Andrew Wheatcroft, 1986.
- (3) A Quick & Dirty Guide to War. James E. Dunnigan and Austin Bay, 1986.
- (4) Atlas of the Third World. George Kurian, 1983.
- (5) Hammond World Atlas. 1984, Hammond Inc.
- (6) Countries of the World and Their Leaders Yearbook 1989. Gale Research, Inc.
- (7) Worldmark Encyclopedia of the Nations. 1984, Worldmark Press Inc.
- (8) USMC Intelligence Center document titled Trafficability Narrative.

### SUMMARY ASSESSMENT OF IMPACT ON EXPEDITIONARY ENVIRONMENT COUNTRIES

The accompanying matrix shows the regional distribution of countries according to their degree of intervisibility. In the Western Hemisphere, over 80 percent of the countries have poor intervisibility where armor and antiarmor weapons cannot be fully employed. Only Cuba, Mexico, and Venezuela could accommodate better line of sight ranges.

In the Middle East/Southwest Asia, more than half the countries had poor intervisibility. The exceptions here were the flat and barren countries of Egypt, Kuwait, Qatar, and the United Arab Emirates, and to a lesser extent Iraq and Libya which had better line of sight distances.

In Africa, 60 percent of the countries had average line of sight distances less than 1,000 meters. Kenya and Tunisia could accommodate intervisibility between 1,000 and 2,000 meters while Algeria, Djibouti, Ethiopia, and Somalia could exceed 2,000 meters.

The great majority of countries in Asia/Pacific and Europe/Mediterranean fall into the category of poor intervisibility. In the middle category on the matrix, with average line of sight ranges between 1,000 and 2,000 meters were found the Asian countries of India and Pakistan and the European country of Denmark.

# REGIONAL DISTRIBUTION OF COUNTRIES BY INTERVISIBILITY

	> 2,000 METERS	1,000 - 2,000 METERS	< 1,000 METERS
WESTERN HEMISPHERE		CUBA	COLOMBIA
		MEXICO	COSTA RICA
		VENEZUELA	EL SALVADOR
			GRENADA
			GUATEMALA
			HAITI
			HONDURAS
			JAMAICA
			NICARAGUA
			PANAMA
			PERU
MIDDLE EAST/ SOUTHWEST ASIA	EGYPT	IRAQ	SAUDI ARAB
	KUWAIT	LIBYA	IRAN
	QATAR		LEBANON
	UAE		NORTH YEMEN
			OMAN
			SAUDI ARABIA
			SOUTH YEMEN
			SYRIA
	ALGERIA	KENYA	ANGOLA
	CHAD	TUNISIA	LIBERIA
AFRICA	ETHIOPIA		MADAGASCAR
	SOMALIA		NAMIBIA
			SOUTH AFRICA
			SUDAN
			UGANDA
			ZAMBIA
			ZIMBABWE
		INDIA	AFGHANISTAN
		PAKISTAN	BANGLADESH
			BURMA
ASIA/ PACIFIC			INDONESIA
			JAPAN
			MALAYSIA
			NORTH KOREA
			PAPUA N. G.
			PHILIPPINES
			ROC
			SOUTH KOREA
			S. PACIFIC IS.
			SRI LANKA
			THAILAND
			VIETNAM
EUROPE/ MED		DENMARK	GREECE
			ITALY
			NORWAY
			TURKEY
			YUGOSLAVIA

## PLANNING AND PROGRAMMING IMPLICATIONS

An overall assessment of intervisibility in the expeditionary environment indicates that almost three quarters of the countries have average line of sight distances less than 1,000 meters. It was determined that on an average the engagement range for armor and antiarmor weapons was about 900 meters. This means that most of the countries in the expeditionary environment have terrain, vegetation, and/or other conditions of obscuration which would preclude engagements by these weapons at their maximum ranges. As a result, it may not be cost effective to acquire and maintain a sizeable number of these weapons in the Marine Corps inventory if they cannot be fully utilized. Light infantry forces with a minimum of armor and heavy equipment would appear to be better able to operate in the restricted terrain and visibility conditions that were identified in this assessment. Manne planners must continually evaluate the tradeoffs between forces and weapon systems to select those that can be employed most effectively in the anticipated environment.

Mission Area Factors - 34

## HYDROGRAPHY - NAVAL GUNFIRE CONSTRAINTS

### CRITERIA FOR LEVELS OF DIFFICULTY

Hydrography - NGF Constraints	LEVELS OF DIFFICULTY			
	Good	Fair	Poor	Unsatisfactory

**UNSATISFACTORY:** Distance of the 5 Fathom Line from the coast is greater than 24,000 meters

**POOR:** Distance of the 5 Fathom Line from the coast is between 16,001 and 24,000 meters

**FAIR:** Distance of the 5 Fathom Line from the coast is between 8,001 and 16,000 meters

**GOOD:** Distance of the 5 Fathom Line from the coast is 8,000 meters or less

This assessment addresses NGF capabilities and the constraints imposed by hydrographic conditions off the coasts of expeditionary environment countries. For purposes of this evaluation, a U.S. Navy destroyer with an 8.8 meter (29 foot) draft and 5-inch 54-caliber guns was chosen as the representative NGF platform. To determine coastal hydrographic conditions, the Defense Mapping Agency's hydrographic charts were examined to identify the closest distance a destroyer could operate offshore of the countries of interest. Because the water depths and conditions along extended coastlines frequently have significant variations, key locations (adjacent to ports, cities, or key lines of communications inland) where an ATF would be likely to operate were selected, and a reading taken of the average distance of the 5 Fathom Line from the coast. (Distances were calculated only to the beach, not to inland targets.) Distances were then compared with the 24,000 meter maximum range of the destroyer's guns and a NGF rating based on the above scale was assigned to each country. Volume II, Study Supporting Material, Section 23. Hydrography - Naval Gunfire Constraints provides a listing of country key locations selected for a reading of the 5 Fathom Line, DMA chart numbers of charts used, the assessed distance of the 5 Fathom Line from the coast and the overall country ratings. The primary reference used for this assessment was the Department of Defense, Defense Mapping Agency, Catalog of Maps, Charts, and Related Products, Part 2 - Hydrographic Products.

### SUMMARY ASSESSMENT OF IMPACT ON EXPEDITIONARY ENVIRONMENT COUNTRIES

The accompanying charts show a regional breakdown of NGF capabilities affected by hydrography. In the Western Hemisphere, most of the countries have conditions favorable to NGF coverage. Only Surinam had unsatisfactory conditions which would prevent the use of NGF.

### NAVAL GUNFIRE CAPABILITIES BY REGION

		GOOD	FAIR	POOR	UNSATISFACTORY
WESTERN HEMISPHERE	COLOMBIA		HONDURAS		SURINAM
	COSTA RICA				
	CUBA				
	DOM. REP.				
	EL SALVADOR				
	GRENADA				
	GUATEMALA				
	HAITI				
	JAMAICA				
	MEXICO				
	NICARAGUA				
	PANAMA				
	PERU				
	VENEZUELA				

Mission Area Factors - 35



In the Middle East/Southwest Asia, NGF can be employed to various degrees of effectiveness in all the countries. Iraq and North Yemen were found not to have the poorest conditions.

In Africa, hydrographic conditions were not identified as limiting NGF employment. Only against the inland countries of Uganda and Zimbabwe was it found not feasible to use NGF.

In Asia/Pacific there was determined to be a range of conditions. Due to the offshore constraints involved, NGF could not be effectively employed in Bangladesh, Burma, North Korea, and the People's Republic of China, as well as the inland country of Afghanistan. In other countries in this region, NGF could be delivered with varying degrees of effectiveness.

In Europe/Mediterranean offshore hydrographic conditions were found to permit satisfactory NGF coverage in all of the six countries considered.

#### NAVAL GUNFIRE CAPABILITIES BY REGION

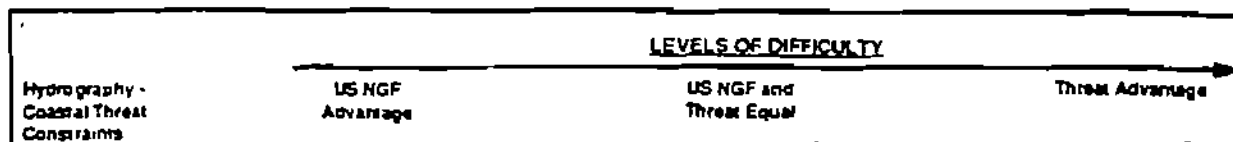
	GOOD	FAIR	POOR	UNSATISFACTORY
MIDDLE EAST/SOUTHWEST ASIA	KUWAIT	BAHRAIN	IRAQ	
	LEBANON	EGYPT	NORTH YEMEN	
	OMAN	IRAN		
	SOUTH YEMEN	LIBYA		
	SYRIA	QATAR		
		SALAH ARABIA		
		UAE		
AFRICA	ALGERIA	KENYA		UGANDA
	ANGOLA	MADAGASCAR		ZIMBABWE
	BURUNDI	ZAMBIE		
	ETHIOPIA			
	LIBERIA			
	NAMIBIA			
	SOMALIA			
	SOUTH AFRICA			
	SUDAN			
	TUNISIA			
ASIA/PACIFIC	INDONESIA	INDIA	SOUTH KOREA	AFGHANISTAN
	JAPAN	MALAYSIA		BANGLADESH
	PHILIPPINES	PAKISTAN		BURMA
	S. PACIFIC IS.	PAPUA N. G.		NORTH KOREA
	ERI LANKA			PRC
	THAILAND			
	VIETNAM			
	Note: Hydrographic charts were not available for the Society Islands			
EUROPE/MED	DENMARK			
	GREECE			
	ITALY			
	NORWAY			
	TURKEY			
	YUGOSLAVIA			

#### PLANNING AND PROGRAMMING IMPLICATIONS

The results of this assessment indicate that good NGF coverage is possible in over half of the expeditionary environment countries if a destroyer approaches to its closest point off the beach. However, to execute an Over-The-Horizon (OTH) amphibious assault where the element of surprise is highly important, it is necessary that the NGF platform operate further out to sea and still cover the priority targets ashore. For this type of operation the 24,000 meter range of the 5-inch, 54-caliber gun is no longer satisfactory. To adequately support OTH operations in the future, Marines must encourage and support Navy actions to acquire an NGF weapon with a range of at least 60 nautical miles.

## HYDROGRAPHY - COASTAL THREAT CONSTRAINTS

### CRITERIA FOR LEVELS OF DIFFICULTY



**THREAT ADVANTAGE.** Maximum range of threat coastal defense weapons exceeds 24,000 meters

**US NGF AND THREAT EQUAL.** Maximum range of threat coastal defense weapons is 24,000 meters

**US NGF ADVANTAGE:** Maximum range of threat coastal defense weapons is less than 24,000 meters

This assessment considers U.S. NGF capabilities as compared to the effectiveness of threat surface-to-surface weapons when used for coastal defense. For purposes of this evaluation, the representative NGF platform was again a destroyer with 5-inch, 54-caliber guns positioned off the coast of expeditionary environment countries. The maximum range of the 5-inch, 54-caliber gun was considered to be 24,000 meters. The methodology for this assessment involved gathering data on surface-to-surface weapons of the countries of interest and comparing the longest range weapon with that of the U.S. destroyer's 5-inch, 54-caliber gun. The above scale was used to assign a rating or level of difficulty to each country.

Volume II, Study Supporting Material, Section 24, Hydrography - Coastal Threat Constraints contains a listing of each country's maximum capability weapon, each weapon's maximum range, and the country ratings which were assigned. The primary data source used for this assessment was Jane's Weapon Systems, 1987 - 88.

### SUMMARY ASSESSMENT OF IMPACT ON EXPEDITIONARY ENVIRONMENT COUNTRIES

The accompanying charts illustrate a regional breakdown of U.S. NGF versus threat coastal defense capabilities. It was found that the coastal threat may pose a major problem, as 44 percent of the countries considered have at least some capability that exceeds the range of the standard 5-inch gun on most Navy combatants.

In the Western Hemisphere, Cuba, Peru, and Venezuela have a firepower advantage, while Honduras and Nicaragua possess a capability equal to U.S. NGF.

### U.S. NGF VERSUS THREAT CAPABILITIES BY REGION

	U.S. NGF ADVANTAGE	U.S. NGF AND THREAT EQUAL	THREAT ADVANTAGE
WESTERN HEMISPHERE	COLOMBIA	HONDURAS	CUBA
	COSTA RICA	NICARAGUA	PERU
	DOM. REP.		VENEZUELA
	EL SALVADOR		
	GRENADA		
	GUATEMALA		
	HAITI		
	JAMAICA		
	MEXICO		
	PANAMA		
	SURINAM		

In the Middle East/Southwest Asia, over two-thirds of the countries have a firepower advantage over U.S. NGF. It is particularly noteworthy that unstable countries such as Iran, Iraq, and Libya fall into this category.

In Africa, almost half the countries, including Algeria, Angola, Somalia, and Sudan, can out-gun the 5-inch, 54-caliber weapon.

In Asia/Pacific, seven countries have the advantage in firepower, the most notable of which are North Korea, the People's Republic of China, and Vietnam. Thailand was found to have a capability equal to U.S. NGF.

In Europe and the Mediterranean, all the countries considered except Denmark have the advantage against U.S. NGF.

#### U.S. NGF VERSUS THREAT CAPABILITIES BY REGION

	U.S. NGF ADVANTAGE	U.S. NGF AND THREAT EQUAL	THREAT ADVANTAGE
MIDDLE EAST/ SOUTHWEST ASIA	NORTH YEMEN	BAHRAIN	EGYPT
	QATAR		IRAN
	UAE		IRAQ
			KUWAIT
			LEBANON
			LIBYA
			OMAN
			SAUDI ARABIA
			SOUTH YEMEN
			SYRIA
AFRICA	DJIBOUTI		ALGERIA
	KENYA		ANGOLA
	LIBERIA		ETHIOPIA
	NAMIBIA		MADAGASCAR
	SOUTH AFRICA		SOMALIA
	TUNISIA		SUDAN
	ZAMBIE		
ASIA/ PACIFIC	BAHOLADESH	THAILAND	INDIA
	BURMA		JAPAN
	INDONESIA		NORTH KOREA
	MALAYSIA		PAKISTAN
	PAPUA N. G.		PRC
	PHILIPPINES		SOUTH KOREA
	S. PACIFIC IS.		VIETNAM
	SEYSHL IS.		
	SRI LANKA		
EUROPE/ MEDI	DENMARK		GREECE
			ITALY
			NORWAY
			TURKEY
			YUGOSLAVIA

#### PLANNING AND PROGRAMMING IMPLICATIONS

This assessment has found that many of the expeditionary environment countries have acquired surface-to-surface weapons which, when employed in a coastal defense role, would give them the advantage over the standard U.S. NGF capabilities. The 24,000-meter range of the 5-inch, 54-caliber gun is inadequate to provide the necessary support for amphibious or limited objective operations. To effectively suppress enemy coastal defenses and engage inland targets from an Over-The-Horizon (OTH) location a more capable NGF weapon is needed. Marines must encourage and support Navy actions to obtain an enhanced NGF capability that will support expeditionary operations at a range of 60 nautical miles or more.

Mission Area Factors - 38

## MAPPING, CHARTING, AND GEODESY SHORTFALLS

### CRITERIA FOR LEVELS OF DIFFICULTY

	LEVELS OF DIFFICULTY					
	A	B	C	D	E	F
MC&G Coverage	1:50 New	1:50 Old	Some 1:50	MSI Avail	1:250 New	None

**E** - Countries with no coverage by 1:50,000 or 1:250,000 scale maps or Multispectral Imagery (MSI)

**E** - Countries with complete coverage by 1:250,000 scale maps (either series 1501 (ground) or 1501A (air)) and map editions all have been produced since 1980. No 1:50,000 scale map coverage or MSI are available.

**D** - Countries which have current and complete MSI available, but no 1:50,000 scale map coverage

**C** - Countries with partial coverage by either current or dated 1:50,000 scale maps

**B** - Countries with complete coverage by 1:50,000 scale maps, most editions of which were produced prior to 1980

**A** - Countries with complete coverage by 1:50,000 scale maps and all map editions were produced since 1980

Using the above criteria, expeditionary environment countries were classified into the six categories (A through F) through research of the data sources. These sources consisted of the following.

- (1) Department of Defense, Defense Mapping Agency, Catalog of Maps, Charts, and Related Products
- (2) Telephone conversations with the Earth Observation Satellite Company, Subject: MSI Support for DMA
- (3) Commanding General, Marine Corps Combat Development Command letter 3140 IN 06 dated June 1, 1989, Subject: Marine Corps Concerns--Mapping, Charting, and Geodesy Documents.

### SUMMARY ASSESSMENT OF IMPACT ON EXPEDITIONARY ENVIRONMENT COUNTRIES

The accompanying charts show the distribution of Mapping, Charting, and Geodesy (MC&G) coverage by region. Because there was no countries identified with items E (1:250 New) and F (None) at the upper end of the level of difficulty scale, these items were not addressed further in this assessment.

In the Western Hemisphere, only four countries had full coverage by the older 1:50,000 scale maps. These were Cuba, Dominican Republic, Haiti and Jamaica. Over 50 percent of the countries had partial coverage with 1:50,000 maps while Grenada, Mexico, and Surinam had the less effective MSI available.

#### DISTRIBUTION OF COUNTRIES BY MC&G COVERAGE

	1:50 NEW	1:50 OLD	SOME 1:50	MSI AVAIL
WESTERN HEMISPHERE		CUBA DOM. REP. HAITI JAMAICA	COLOMBIA COSTA RICA EL SALVADOR GUATEMALA HONDURAS NICARAGUA PANAMA PERU VENEZUELA	GRENADA MEXICO SURINAM

In the Middle East/Southwest Asia most of the countries had some 1:50,000 scale map coverage. Only Bahrain had full coverage with dated 1:50,000 maps, and Kuwait and North Yemen had just the MSI available.

In Africa, there were no countries with full 1:50,000 scale map coverage. Countries in this region were about equally divided between those with partial coverage by 1:50,000 scale maps and those with MSI. Countries such as Algeria, Liberia, South Africa, and Zimbabwe had partial 1:50,000 map coverage. Representative countries with only MSI were Angola, Namibia, Sudan, and Uganda.

In the Asia/Pacific region there were only two countries, North Korea and South Korea, with full coverage by dated 1:50,000 scale maps. The remaining countries were equally divided between the partial 1:50 and the MSI available categories. Nations such as Afghanistan, Pakistan, and Thailand had the partial 1:50 while Burma, India, and Malaysia were representative of the MSI available category.

In Europe and the Mediterranean, the countries of Greece and Turkey presented the most difficult conditions with only MSI available. Italy has partial 1:50 coverage while Denmark, Norway and Yugoslavia had full coverage with the dated 1:50's.

**DISTRIBUTION OF COUNTRIES BY MC&G COVERAGE**

	1:50 NEW	1:50 OLD	SOME 1:50	MSI AVAIL
MIDDLE EAST/ SOUTHWEST ASIA		BAHRAIN	EGYPT IRAN IRAQ LEBANON LIBYA OMAN QATAR SAUDI ARABIA SOUTH YEMEN SYRIA UAE	KUWAIT NORTH YEMEN
AFRICA			ALGERIA DJIBOUTI ETHIOPIA LIBERIA SOUTH AFRICA TUNISIA ZAIRE ZIMBABWE	ANGOLA KENYA MADAGASCAR NAMIBIA SOMALIA SUDAN UGANDA
ASIA/PACIFIC		NORTH KOREA SOUTH KOREA	AFGHANISTAN INDONESIA JAPAN PAKISTAN PHILIPPINES PRC THAILAND VIETNAM	BANGLADESH BURMA INDIA MALAYSIA PAPUA N. G. S. PACIFIC IS. SPRATLY IS. SRI LANKA
EUROPE/MED		DENMARK NORWAY YUGOSLAVIA	ITALY	GREECE TURKEY

#### **PLANNING AND PROGRAMMING IMPLICATIONS**

This assessment has indicated that there are significant shortfalls in MC&G coverage of expeditionary environment countries. Over 85 percent of the countries have only partial 1:50,000 scale map coverage or MSI. As a result of this situation, MAGTF's employed in many of these countries will not have the maps required to conduct effective ground and air operations. To overcome this deficiency, actions must be taken to ensure that the Defense Mapping Agency directs its available resources toward an aggressive large-scale mapping program of Third World countries to support the range of operations across the spectrum of conflict.

Mission Area Factors - 40

## AIRFIELDS

### CRITERIA FOR LEVELS OF DIFFICULTY

	LEVELS OF DIFFICULTY					
	A	B	C	D	E	F
Airfields	>1 C-5	1 C-5	2-3 C-130	2-4 C-130	1 C-130	None

- F** - Countries with no airfields that are capable of receiving C-130 or larger transport aircraft
- E** - Countries with only one airfield that can accommodate C-130 or C-141B aircraft. There are no airfields that can receive C-5 aircraft.
- D** - Countries with two to four airfields that can accommodate C-130 or C-141B aircraft. There are no airfields that can receive C-5 aircraft.
- C** - Countries with five or more airfields that can accommodate C-130 or C-141B aircraft. There are no airfields that can receive C-5 aircraft
- B** - Countries with only one airfield that can receive C-5 aircraft. These countries may have additional airfields that can handle C-141B and C-130 aircraft.
- A** - Countries with more than one airfield that can receive C-5 aircraft. These countries may also have airfields that can handle only C-141B and C-130 aircraft.

Using the above criteria, in conjunction with a thorough review of source material, the expeditionary environment countries were classified into the six levels of difficulty (A to F). The purpose in this instance was to show the degree of access that a military force might have to a country through its airfields. Volume II, Study Supporting Material, Section 26, Airfields contains a listing of the primary airfields in each country, a brief description of each airfield and the overall country rating assigned. The principal reference used for source material was the Military Air Command, Code DOVF, Airfield Suitability Report, dated August 1, 1969.

### SUMMARY ASSESSMENT OF IMPACT ON EXPEDITIONARY ENVIRONMENT COUNTRIES

The accompanying chart shows a breakdown of countries by their capability to receive strategic airlift. Overall nearly 80 percent of the countries have at least one airfield that can receive C-5s. There are more than one C-5 capable airfields in 50 percent of the countries. Some of the airfields, however, are constrained in such ways as runway condition, ramp space, fuel storage, and other support functions.

In the **Western Hemisphere**, all the countries considered have at least one airfield able to receive C-5 aircraft. Particularly noteworthy are **Colombia** with 3 C-5, 4 C-141B, and 2 C-130 capable airfields, and **Honduras** with 3 C-5 and 7 C-130 capable airfields.

In the **Middle East/Southwest Asia** 10 of 14 countries or over 70 percent of the total, have at least one airfield which will accommodate C-5s. **Saudi Arabia** has 9 C-5 capable airfields while **Iran** has 8 and **Egypt** 6. In this region, **Iraq**, **North Yemen**, and **Qatar** all have the least accessibility to airlift with only one C-141B capable airfield.

**Africa** has the fewest countries with airfields able to handle large transport aircraft. The six countries of **Algeria**, **Angola**, **Madagascar**, **Tunisia**, **Uganda**, and **Djibouti** are all unable to accommodate C-5s.

In **Asia/Pacific**, 11 of 18 countries have more than one airfield that can receive C-5s and 4 of 18 countries have just one airfield with this capability. Only **Afghanistan** and **Burma** are limited to C-141B capable airfields while no airfields for transport aircraft can be found in the **Spratty Islands**.

In **Europe and the Mediterranean**, 5 of 6 countries have more than one C-5 capable airfield. Only **Yugoslavia** has the lesser capability of 4 C-141B capable airfields.

## AIRFIELDS

	>1/C-5	1/C-5	>5C-130	2-4/C-130	1/C-130	NONE
WESTERN HEMISPHERE	COLOMBIA	COSTA RICA				
	DOM. REP	CUBA				
	GUATEMALA	EL SALVADOR				
	HONDURAS	GRENADA				
	JAMAICA	HAITI				
	MEXICO	NICARAGUA				
	PANAMA	PERU				
	VENEZUELA	SURINAM				
MIDDLE EAST/ SOUTHWEST/ ASIA	EGYPT	BAHRAIN		LIBYA	IRAQ	
	IRAN	KUWAIT			NORTH YEMEN	
	OMAN	LEBANON			QATAR	
	SAUDI ARABIA	SOUTH YEMEN				
	UAE	SYRIA				
AFRICA	ETHIOPIA	LIBERIA	ALGERIA	TUNISIA	DJIBOUTI	
	KENYA	NAMIBIA	ANGOLA	UGANDA		
	SOMALIA	SOUTH AFRICA	MADAGASCAR			
	SUDAN	ZIMBABWE				
	ZAIRE					
ASIA/ PACIFIC	INDIA	BANGLADESH		AFGHANISTAN		SPRATLY IS.
	INDONESIA	PAPUA N. G.		BURMA		
	JAPAN	S. PACIFIC IS.				
	MALAYSIA	SRI LANKA				
	NORTH KOREA					
	PAKISTAN					
	PHILIPPINES					
	PRC					
	SOUTH KOREA					
	THAILAND					
	VIETNAM					
EUROPE/ MED	DENMARK		YUGOSLAVIA			
	GREECE					
	ITALY					
	NORWAY					
	TURKEY					

### PLANNING AND PROGRAMMING IMPLICATIONS

The information shown here is designed to illustrate the types of airfields available for planning purposes and provide indicators about where accessibility by strategic airlift may be most difficult. It is noteworthy that strategic airlift (the C-5) surfaced as a very viable option for 79 percent of the countries with tactical airlift (the C-130) opening an additional 21 percent of the countries, if third party nations were available as staging areas. Also, in those cases where direct entry into a country through its airfields is constrained, planners will need to consider access via adjacent countries in conjunction with other tactical means of transport such as helicopter and surface lift.

Mission Area Factors - 42

## PORTS

### CRITERIA FOR LEVELS OF DIFFICULTY

LEVELS OF DIFFICULTY						
	A	B	C	D	E	F
Ports	Wide Harbor/ ≥50' Depth	Wide Harbor/ ≥40' Depth	≥40' Depth	35-39' Depth	25-34' Depth	None

**F** - Countries with no major ports.

**E** - Countries having at least one major port with a large, medium, or small harbor, and channel and anchorage depths of between 25 and 34 feet.

**D** - Countries having at least one major port with a large, medium, or small harbor, and channel and anchorage depths of between 35 and 39 feet.

**C** - Countries having at least one major port with a small harbor, and both channel and anchorage depths exceed 40 feet.

**B** - Countries having at least one major port with either a large or medium harbor, and both channel and anchorage depths between 40 and 50 feet.

**A** - Countries having at least one major port with either a large or medium harbor, and both channel and anchorage depths greater than 50 feet.

#### MAJOR PORT:

- Accommodates vessels over 500 feet in length
- Channel and anchorage depths of 25 feet or more
- Harbor size of large, medium or small

#### HARBOR SIZE:

- Determined by the DMA World Port Index
- Based on area, facilities and wharf space

Through application of the above criteria to the source material, the countries of interest were classified into the six levels of difficulty (A to F). The purpose here was to show the degree of access that a military force might have to a country through its ports. Volume II, Study Supporting Material, Section 27, Ports contains a listing of the primary ports in each country; identifies the most accessible ports; briefly describes each port; and provides overall level of difficulty country ratings. The following references were used for source material:

- (1) Defense Mapping Agency Hydrographic/Topographic Center, World Port Index, Ninth Edition, 1984
- (2) Commander in Chief, U.S. Atlantic Fleet and Commanding General, Marine Corps Combat Development Command, TACMEMO PZ005700-1-88, Deployment of the Assault Follow-On Echelon, June 1988

### SUMMARY ASSESSMENT OF IMPACT ON EXPEDITIONARY ENVIRONMENT COUNTRIES

The accompanying chart shows a breakdown of countries by their capability to receive strategic sealift. Overall, it was found that 33 of 69 countries or about 48 percent of the total fall into the top three levels of difficulty. There were 10 countries, or 14 percent, which have no acceptable major ports. Such countries as El Salvador, Somalia, Oman, and Bangladesh were in this most difficult category. A total of 15 countries, or 22 percent of the expeditionary environment were in the second most difficult category where major ports had channel and anchorage depths of only 25 to 34 feet. Representative countries in this category were Cuba, Nicaragua, Iraq, and Libya. Channel and anchorage depths below 35 feet are highly marginal for the approach and off-load of strategic sealift such as the Maritime Prepositioning Ships (MPS) and other Military Sealift Command (MSC) shipping. MPS ships have drafts up to 33 feet. Certain types of MSC and U.S. Flag Fleet cargo ships have drafts over 40 feet.



From a regional perspective, the Western Hemisphere countries had the fewest suitable ports while Europe and the Mediterranean had countries with the most capable ports. Other regions had a fairly even distribution across the levels of difficulty.

## PORTS

	WIDE/>50'	WIDE/>40'	>40'	35-39'	25-34'	NONE
WESTERN HEMISPHERE			COLOMBIA	JAMAICA	COSTA RICA	EL SALVADOR
			GRENADA	VENEZUELA	CUBA	SURINAM
			MEXICO		DOM REP	
			PANAMA		GUATEMALA	
			PERU		HAITI	
					HONDURAS	
					NICARAGUA	
MIDDLE EAST/ SOUTHWEST ASIA	LEBANON		BAHRAIN	QATAR	IRAQ	NORTH YEMEN
	SAUDI ARABIA		EGYPT		LIBYA	OMAN
	UAE		IRAN			
			KUWAIT			
			SOUTH YEMEN			
			SYRIA			
AFRICA	SOUTH AFRICA	ALGERIA	ANGOLA	DJIBOUTI	MADAGASCAR	SOMALIA
			KENYA	ETHIOPIA	NAMIBIA	UGANDA
			LIBERIA	SUDAN	ZAIRE	ZIMBABWE
				TUNISIA		
ASIA/ PACIFIC	JAPAN		INDIA	NORTH KOREA	BURMA	AFGHANISTAN
	SRI LANKA		INDONESIA		PAKISTAN	BANGLADESH
			MALAYSIA		THAILAND	SPRATLY IS.
			PAPUA N. G.			
			PHILIPPINES			
			PRC			
			SOUTH KOREA			
			S. PACIFIC IS.			
			VIETNAM			
EUROPE/ MED	ITALY		DENMARK			
	NORWAY		GREECE			
	YUGOSLAVIA		TURKEY			

## PLANNING AND PROGRAMMING IMPLICATIONS

The information shown here is designed to illustrate the types of ports available for planning purposes and provide indicators concerning those countries where accessibility by strategic sealift is most difficult. In the process of rapid mission planning for contingency operations in expeditionary countries, Marine Corps planners must be able to examine all avenues of entry, including sea, air, and land and choose the one most effective. Marine Corps wargaming initiatives and other training efforts should be designed to support this process.

## KEY INSTALLATIONS

### CRITERIA FOR LEVELS OF DIFFICULTY

	LEVELS OF DIFFICULTY					
	A	B	C	D	E	F
Key Installations	None	Few Sites	Multi Sites	Pipeline	Oil Field	NBC

- F** - Countries associated with Nuclear, Biological, and Chemical (NBC) weapon possession and production. These countries have NBC production and storage facilities which could present significant industrial complexity in terms of neutralization.
- E** - Countries with oil as a significant natural resource. These countries have oil fields, off-shore oil recovery facilities, and supporting industrial capabilities.
- D** - Countries with numerous industrial complexes together with pipelines for crude oil, refined products, or natural gas.
- C** - Countries with several basic industrial centers in being or under development and moderately capable transportation and communications systems.
- B** - Countries having an underdeveloped infrastructure with only a few important facilities such as airfields, ports, and communications sites.
- A** - No installations of military significance.

Using the above criteria, expeditionary environment countries were classified into the six categories (A through F) through research of the data sources. The purpose here was to show the level of industrial complexity which might be encountered by military forces when operating in a country. Key installations may quickly become priority targets or key objectives when a crisis situation develops. Volume II, Study Supporting Material, Section 28, Key Installations depicts the primary facilities in each country and is the basis for the country ratings assigned. The following references were used for source material:

- (1) Foreign Area Studies, The American University, Area Handbook Series, 1979 - 1989
- (2) Countries of the World and Their Leaders Yearbook, 1989 Gale Research, Inc.
- (3) World Almanac and Book of Facts, 1989.

### SUMMARY ASSESSMENT OF IMPACT ON EXPEDITIONARY ENVIRONMENT COUNTRIES

The accompanying chart shows the distribution of countries according to their degree of industrial complexity. Overall, there were 17 of the 69 countries, or 25 percent, which were identified as having NBC facilities, the most difficult category. An additional 19 countries or 28 percent, had oil fields and supporting industrial capabilities.

From a regional perspective, the **Western Hemisphere** countries showed a range of key installation categories from **Grenada** and **Surinam** with just a few sites, to **Cuba** with a reported chemical and biological capability.

The **Middle East** countries all had numerous communications and transportation facilities as well as pipelines and oil fields. **Egypt**, **Iran**, **Iraq**, **Libya**, and **Syria** were associated with NBC production or possession.

In **Africa**, there again was a range of countries from **Djibouti** and **Liberia** with just a few less developed facilities to **South Africa** with a reported emerging nuclear capability.

In **Asia** there were ten expeditionary environment countries which reportedly produce or possess various types of NBC weapons. These included **India**, **North Korea**, **Pakistan**, and **Vietnam**.

The countries of **Europe** all had modern communications and transportation facilities, including industrial centers and pipelines. **Greece** and **Norway** had offshore oil extraction facilities.

## KEY INSTALLATIONS

	NONE	FEW SITES	MULTIPLE SITES	PIPELINE	OIL FIELD	NBC
WESTERN HEMISPHERE		GRENADA	EL SALVADOR	COSTA RICA	COLOMBIA	CUBA
		SURINAM	HAITI	DOM REP	GUATEMALA	
			HONDURAS	JAMAICA	MEXICO	
				NICARAGUA	PERU	
				PANAMA	VENEZUELA	
MIDDLE EAST/ SOUTHWEST ASIA				LEBANON	BAHRAIN	EGYPT
				SOUTH YEMEN	KUWAIT	IRAN
					NORTH YEMEN	IRAQ
					OMAN	LIBYA
					QATAR	SYRIA
					SAUDI ARABIA	
AFRICA					UAE	
		DJIBOUTI	ETHIOPIA	KENYA	ALGERIA	SOUTH AFRICA
		LIBERIA	MADAGASCAR	SOMALIA	ANGOLA	
			NAMIBIA	SUDAN	TUNISIA	
			UGANDA	ZAIRE		
ASIA/ PACIFIC			ZIMBABWE			
	SPRATLY IS.	S. PACIFIC IS.	PAPUA N. G.	BANGLADESH	AFGHANISTAN	BURMA
				PHILIPPINES	MALAYSIA	INDIA
				SRI LANKA		INDONESIA
						JAPAN
						NORTH KOREA
						PAKISTAN
						PRC
						SOUTH KOREA
						THAILAND
						VIETNAM
EUROPE/ MED				DENMARK	GREECE	
				ITALY	NORWAY	
				TURKEY		
				YUGOSLAVIA		

### PLANNING AND PROGRAMMING IMPLICATIONS

This assessment has indicated that there is a wide diversity of industrial complexity among the countries of interest. Marines must have an understanding of the infrastructure within these countries to be prepared for a range of operations across the spectrum of conflict. Because events frequently unfold very quickly, important facilities in a country can suddenly become key objectives for peacetime contingency or counterterrorism operations. NBC weapons producing facilities may need to be rapidly seized and secured without adverse affect. Ports and airfields may need to be neutralized and then rapidly repaired so they can be used by friendly forces. Noncombat equipment material, and replacement parts will all be required to complete this process satisfactorily. Manne planners must ensure that equipment acquisition and training actions are taken to achieve the maximum level of readiness for these situations. Marines, and especially their engineers, must know how such facilities are constructed, what key nodes are within the facilities, and how to protect, destroy, or covertly neutralize the facility.

Mission Area Factors - 46

## STRATEGIC AND TACTICAL LIFT CAPABILITIES AND CONSTRAINTS

### CRITERIA FOR LEVELS OF DIFFICULTY

MEU Response Time	LEVELS OF DIFFICULTY			
	A	B	C	D
	<2 Days	≥2 - <4 Days	≥4 - <6 Days	≥6 Days

**D** - Countries which require more than 6 days deployment time for a sea-based MEU.

**C** - Countries which require between 4 to 6 days deployment time for a sea-based MEU.

**B** - Countries which require between 2 and 4 days deployment time for a sea-based MEU.

**A** - Countries which require less than 2 days deployment time for a sea-based MEU.

### GUIDELINES

- (1) The focus was on typical response times for forward-deployed MEUs and garrison MEUs on the U.S. east and west coasts. The Air Alert Force (AAF) and two Air Contingency Battalions (ACBs) were recognized as a capability to deploy Marines by strategic airlift to any location in the world within 24 hours. However, because neither the AAF nor the ACBs possess a forcible entry capability, they were not factored into this assessment.
- (2) The Atlantic Amphibious Ready Group (ARG) with an embarked MEU normally operates in the Mediterranean Sea. The Pacific ARG with its embarked MEU operates either in the Middle East/Southwest Asia region or the Western Pacific based on intelligence reports and the anticipated threat. An assumption was made that there would be some advance warning of a developing crisis to allow initial movement of the ARGs toward an objective area.
- (3) Garrison MEUs at Camp Lejeune and Camp Pendleton both require 72 hours to embark aboard amphibious ships. Once embarked, it would require 3 more days for the Atlantic coast MEU to reach the Caribbean Sea and the Pacific coast MEU to reach the southern part of Mexico.
- (4) ARGs, once underway, would maintain a speed of 12 knots.

Using the above methodology in conjunction with the data sources, the countries of interest were placed in the four categories (A through D). The following references were used as the basis for this assessment.

- (1) Defense Mapping Agency, Hydrographic/Topographic Center, Distance Between Ports, Fifth Edition, 1985.
- (2) MAGTF Warfighting Center letter dated 13 November 1989, Subject: Deployment Capabilities Guidelines.
- (3) Headquarters U.S. Marine Corps, Marine Air-Ground Task Force Master Plan, dated 7 July 1989.

### SUMMARY ASSESSMENT OF IMPACT ON EXPEDITIONARY ENVIRONMENT COUNTRIES

The accompanying charts show the regional distribution of expeditionary environment countries according to their respective sea-based MEU response times. In the Western Hemisphere, most of the countries require in excess of 6 days deployment time. Only a portion of Mexico and Cuba can be reached in less time. This is due to the time necessary for garrison MEUs on the U.S. east and west coasts to embark on amphibious ships and sail to these countries. In the Middle East/Southwest Asia, however, ARG/MEU arrival times at most countries are less than 2 days. These countries are mainly on the Mediterranean Sea and Persian Gulf littoral and are in proximity to the principal ARG/MEU operating areas. In Africa, over half the countries required a response time of more than 6 days. These countries are outside the Mediterranean Sea and the farthest away from the ARG/MEU operating in the Indian Ocean. In Asia/Pacific, response times were calculated from a likely ARG/MEU operating area in the Philippines. Those countries most distant from the Philippines had the longest response times. In Europe/Mediterranean, the countries of Norway and Denmark had the longest response times for the ARG/MEU operating primarily in the Mediterranean Sea.

# **DISTRIBUTION OF COUNTRIES BY ARG/MEU RESPONSE TIMES**

	< 2 DAYS	> 2 < 4 DAYS	> 4 < 6 DAYS	> 6 DAYS
WESTERN HEMISPHERE		NORTH MEXICO	CUBA MID-MEXICO	COLOMBIA COSTA RICA DOM. REP. EL SALVADOR GRENADA GUATEMALA HAITI HONDURAS JAMAICA SOUTH MEXICO NICARAGUA PANAMA PERU SURINAM VENEZUELA
MIDDLE EAST/ SOUTHWEST ASIA	BAHRAIN EGYPT IRAN IRAQ KUWAIT LEBANON LIBYA OMAN QATAR SAUDI ARABIA SYRIA UAE	NORTH YEMEN SOUTH YEMEN		
AFRICA	ALGERIA TUNISIA	DJIBOUTI	KENYA MADAGASCAR SOMALIA	ANGOLA ETHIOPIA LIBERIA NAMIBIA SOUTH AFRICA SUDAN UGANDA ZAIRE ZIMBABWE
ASIAPACIFIC	COASTAL INDIA COASTAL PAKISTAN PHILIPPINES SPRATLY IS.	INLAND INDIA INDONESIA MALAYSIA INLAND PAKISTAN PAPUA N. GUINEA COASTAL PRC SRI LANKA THAILAND VIETNAM	BANGLADESH BURMA SOUTHERN JAPAN INLAND PRC SOUTH KOREA S. PACIFIC IS. (SOLOMON IS.)	AFGHANISTAN NORTHERN JAPAN NORTH KOREA S. PACIFIC IS. (FIJI, KIRIBATI, VANUATU)
EUROPE/MED	GREECE ITALY TURKEY YUGOSLAVIA		DENMARK	NORWAY

## **PLANNING AND PROGRAMMING IMPLICATIONS**

This assessment has found that 42 percent of the countries have ARG/MEU response times of more than six days. This suggests that the Commandant's recent emphasis on strategic deployment by air merits in-depth planning and programming support. In the area of tactical lift, capabilities such as the Landing Craft Air Cushion (LCAC) will allow a naval expeditionary force to be far offshore and still effectively strike a target. The CH-46 helicopter, however, does not have the extended range to adequately support the OTH assault and a replacement such as the MV-22A Osprey needs to be acquired. By using tactical lift capabilities such as the Advanced Assault Amphibious Vehicle, high-speed LCAC, and extended-range vertical lift, the ATF will have a better opportunity to execute its OTH assault.

## NONCOMBATANT EVACUATION LOGISTICS

### CRITERIA FOR LEVELS OF DIFFICULTY

	LEVELS OF DIFFICULTY					
	A	B	C	D	E	F
NEO						
Embassy Staff	<25	<50	<100	<250	<500	>500
Evacuees	None	<100	<200	<300	>300	>500*
Inland Obj	Coastal	<100 NM	<300 NM	>300 NM	>500 NM	>999 NM

\* For purposes of this study, 500 evacuees was used as a threshold. Anything above 500 would probably require consideration of other options, i.e., evacuation by airlift or sealift.

**F** - U.S. Embassy staff over 500; evacuees over 500; and evacuation site 1,000 nm or more from the coast.

**E** - U.S. Embassy staff - 250 to 500; evacuees - 300 to 500; and evacuation site 500 to 1,000 nm from the coast

**D** - U.S. Embassy staff - 100 to 250; evacuees - 200 to 300; and evacuation site 300 to 500 nm from the coast

**C** - U.S. Embassy staff - 50 to 100; evacuees - 100 to 200; and evacuation site 100 to 300 nm from the coast.

**B** - U.S. Embassy staff - 25 to 50; evacuees - up to 100; and evacuation site up to 100 nm from the coast.

**A** - U.S. Embassy staff less than 25; no evacuees; and evacuation site located on the coast.

**EMBASSY STAFF:** This includes the Country Team and supporting units such as the Marine Security Guard. Not included are Foreign Nationals who under some circumstances would require evacuation.

**EVACUEES:** These are the U.S. citizens (less military personnel and U.S. Embassy staff) in residence.

**INLAND OBJECTIVE:** The capital of each country was selected as the NEO inland objective (evacuation site). Distances were calculated from a point just off the coast to the capital.

Using the above criteria in conjunction with source material, the countries of interest were assigned a rating (A through F). Because a number of countries did not always match the designated categories for Embassy Staff, Evacuees, and Inland Obj, the highest value for the three categories determined the rating. For example, if the country's evacuees exceeded 500 but the inland objective was less than 200 nm from the coast, an "F" rating was assigned. Volume II, Study Supporting Material, Section 30, Noncombatant Evacuation Logistics contains the data for each country on which the ratings are based. The following references were used as source material:

- (1) U.S. Department of State, Statistics on U.S. Embassies in Countries of Interest, 21 February 1990.
- (2) U.S. Department of State, Numbers of U.S. Citizens Living in Countries of Interest, 21-22 February 1990.

### SUMMARY ASSESSMENT OF IMPACT ON EXPEDITIONARY ENVIRONMENT COUNTRIES

The accompanying chart shows the regional distribution of countries according to noncombatant evacuation logistics. In the Western Hemisphere, over 80 percent of the countries fell into the most difficult category due primarily to the large number of potential evacuees.

In the Middle East/Southwest Asia, all but two countries were rated in the three most difficult categories. There were 9 of the 16 countries in this region that had more than 500 potential evacuees while 5 countries had distances to their capitals (evacuation points) exceeding the range (70 nautical miles) of the CH-46 medium lift helicopter.

In Africa, over half the countries presented the most difficult logistic conditions for NEO. Nine of the 15 countries in this region had evacuation distances greater than the range of the CH-46.

In Asia/Pacific a total of 12 countries were in the most difficult category while in Europe/Mediterranean all 6 countries were rated most difficult. These two regions had 7 countries where distances to the evacuation point exceeded the range of the CH-46. There were 18 countries in these regions with more than 500 evacuees.

**REGIONAL DISTRIBUTION OF COUNTRIES BY NONCOMBATANT  
EVACUATION LOGISTICS  
INCREASING DIFFICULTY**

WESTERN HEMISPHERE			EL SALVADOR	CUBA SURINAM		COLOMBIA COSTA RICA DOM. REP. GRENADA GUATEMALA HAITI HONDURAS JAMAICA MEXICO NICARAGUA PANAMA PERU VENEZUELA
MIDDLE EAST/ SOUTHWEST ASIA	LIBYA SOUTH YEMEN			IRAN IRAQ	QATAR	BAHRAIN EGYPT KUWAIT LEBANON NORTH YEMEN OMAN SAUDI ARABIA SYRIA UAE
AFRICA	ANGOLA	DJIBOUTI	MADAGASCAR NAMIBIA	SOMALIA	ALGERIA UGANDA	ETHIOPIA KENYA LIBERIA SOUTH AFRICA SUDAN TUNISIA ZAIRE ZIMBABWE
ASIA/PACIFIC	SPRATLY IS.	NORTH KOREA VIETNAM	BURMA		AFGHANISTAN S. PACIFIC IS.	BANGLADESH INDIA INDONESIA JAPAN MALAYSIA PAKISTAN PAPUA N. GUINEA PHILIPPINES PRC SOUTH KOREA SRI LANKA THAILAND
EUROPE/MED						DENMARK GREECE ITALY NORWAY TURKEY YUGOSLAVIA

**PLANNING AND PROGRAMMING IMPLICATIONS**

Despite the emphasis in recent years on the importance of the MAGTF in NEO, the study found that these operations are extremely difficult in 53 of the 69 countries (77%) unless there is a major draw-down of U.S. citizens before the crisis develops, or provisions are made for the use of strategic airlift to evacuate the noncombatants. The existing range and lift capability of the CH-46 cannot support the requirements of the expeditionary environment. In most countries, there are over 100 U.S. citizens in the Embassy, and/or over 200 U.S. citizens in the national capital and/or the distance of the NEO objective from the offshore platform is greater than 300 nautical miles.

Mission Area Factors - 50

## APPENDIX G

### OSINT OPSEC: Selected References and Information

NOTE: The complete addresses for all of the publishers are provided at the end of this handout.

#### OPEN SOURCES AND TELEPHONE INTERCEPTION

Tom Kneitel, *Tune In On Telephone Calls*, CRB Research (1993)  
ISBN: 0-939780-19-4

#### OPEN SOURCES AND RADIO INTERCEPTION

*Monitoring Air Force One*- 50 page manual. Published without any reference to the identity of its author nor to the place or date of its publication. Purchased in July, 1994, through an ad placed in *Monitoring Times*.

Tom Kneitel, *Guide to Embassy & Espionage Communications*, CRB Research (1986).  
ISBN: 0-939780-06-2

Monthly hobbyist magazine: *Monitoring Times*, Brasstown, NC.

#### OPEN SOURCES AND EAVESDROPPING

*Electronic Eavesdropping Techniques and Equipment*, prepared for the National Institute of Law Enforcement and Criminal Justice, Law Enforcement Assistance Administration, U.S. Department of Justice, by Raymond N. Jones. Republished as *Covert Intelligence: Electronic Eavesdropping* by CRB Research. No date listed.

Electronic plans from - *Portfolio of Schematic Diagrams for Electronic Surveillance*, Mentor Publications, Flushing, NY (1979)

#### OPEN SOURCES AND UNDERCOVER OPERATIONS

E. Roy Slade and James R. Gutz, *The Pretext Book*, Cloak and Data Press, Houston, TX (1991). Available through: The P.I. Catalogue, (512) 928-8190.

Kingdon Peter Anderson, *Undercover Operations; A Manual for the Private Investigator*,



Paladin Press (1988). ISBN: 0-87364-486-7.

Eddie the Wire, *The Complete Book of Lockpicking*, Loompanics Unlimited (1981). ISBN: 0-915179-06-7.

Burt Rapp, *Shadowing and Surveillance; A Complete Guidebook*, Loompanics Unlimited (1986). ISBN: 0-915179-33-4.

## OPEN SOURCES AND INTERROGATIONS

Richard W. Krousher, *Physical Interrogation Techniques*. Loompanics Unlimited, (1985). ISBN: 0-915179-23-7.

No author listed, *Interrogations: Techniques and Tricks to Secure Evidence*, Paladin Press (1991). ISBN: 0-87364-625-8.

## OPEN SOURCES AND EXECUTIONS

John Minnery, *How To Kill*, Paladin Press (1973). ISBN: 0-87364-003-9.

George Hayduke, *The Hayduke Silencer Book*, Paladin Press (1989). ISBN: 0-87364-522-7.

John Sanchez, *Slash and Thrust*, Paladin Press (1980). ISBN: 0-87364-188-4.

J. David Turby, *Zips, Pipes, and Pens; A Manual of Improvised Weapons*, Paladin Press (1992). ISBN: 0-87364-702-5.

## OPEN SOURCES AND EXPLOSIVES

Ragnar Benson, *New and Improved C-4*, Paladin Press (1995).

Seymour Lecker, *Homemade Semtex: C-4's Ugly Sister*, Paladin Press (1991). ISBN: 0-87364-617-7.

Thomas Mordechai, *Professional Standards for Preparing, Handling, and Using Explosives*, Paladin Press (1995). ISBN: 0-87364-807-2.

Jo Jo Gonzalez, *Death by Deception; Advanced Improvised Booby Traps*, Paladin Press (1992). ISBN: 0-87364-651-7.

Seymour Lecker, *Improvised Explosives, How To Make Your Own*, Paladin Press (1985).

ISBN: 0-87364-320-8.

No author, *How To Destroy Bridges*, Paladin Press (1988). ISBN: 0-87364-485-9.

#### OPEN SOURCES AND RADIO DETONATION OF BOMBS

Lawrence W. Meyers, *Improvised Radio Detonation Techniques*, Paladin Press (1988). ISBN: 0-87354-479-4.

#### OPEN SOURCES AND VEHICULAR ENHANCEMENTS

Ronald George Eriksen, *Getaway; Driving Techniques For Escape and Evasion*, Loompanics Unlimited (1982)

#### OPEN SOURCES AND TACTICAL COMMUNICATIONS JAMMING

Lawrence W. Myers, *Improvised Radio Jamming Techniques*, Paladin Press (1989). ISBN: 0-87364-520-0.

#### OPEN SOURCES AND BANK CARD FORGERY

Anonymous, *How To Create A New Identity*, Carol Publishing Group, NY (1991). ISBN: 0-8065-1034-X.

Jack Luger, *Counterfeit I.D. Made Easy*, Loompanics Unlimited (1990). ISBN: 0-915179-90-3.

Thomas Collins, *Counterfeit Currency, How To Really Make Money*, Loompanics Unlimited (1990). ISBN: 1-55950-042-5.

John Sample, *Methods of Disguise*, Loompanics Unlimited (1993). ISBN: 1-55950-096-4.

J.F. Straw, *Around The World Contacts*, Worldwide Investment News, Dalton, GA (1991).

#### OPEN SOURCES AND LEGAL OFFSHORE PASSPORTS

*Passport Agent's Manual*, originally published by the U.S. Passport Service, republished by Eden Press, Fountain Valley, CA (no date listed).

## OPEN SOURCES AND CHOOSING A CRIMINAL SPECIALTY

K. Hawkeye Gross, *Drug Smuggling: The Forbidden Book*, Paladin Press (1992).  
ISBN: 0-87364-685-1.

Harold S. Long, *Successful Armed Robbery*, Loompanics Unlimited (1990).  
ISBN: 1-55950-023-9.

Rex Farel, *Hit Man; A Technical Manual for Independent Contractors*, Paladin Press (1992).  
ISBN: 0-87364-7.

Michael Connor, *How To Hide Anything*, Paladin Press (1984).  
ISBN: 0-87364-289-9.

Ragnar Benson, *Gunrunning for Fun & Profit*, Paladin Press (1986).  
ISBN: 0-87364-359-3.

### Communicating with the Publishers

Paladin Press  
P.O. Box 1307  
Boulder, CO 80306  
(800) 392-2400

CRB Research Books, Inc.  
Box 56  
Commack, NY 11725  
(800) 656-0056

Loompanics Unlimited  
P.O. Box 1197  
Port Townsend, WA 98369  
Does not have an (800) order line

Eden Press  
P.O. Box 8410  
Fountain Valley, CA 92728  
(800) 338-8484

For those interested in further study of this topic, catalogues are available from each publisher which document the full range of material available to the public.

### Communicating with the primary source for this lesson:

Mr. Richard Horowitz  
307 West 79th Street  
Suite 331  
New York, NY 10024  
Tel: (212) 362-5199  
Fax: (212) 769-6162  
RHJDPICPT@Compuserve.com

## APPENDIX H

### Countries Comprising the Expeditionary Environment

<u>Asia/Pacific</u>	<u>Europe/Mediterranean</u>	<u>Middle East/SW Asia</u>
Bangladesh	Belarus	Afghanistan
Cambodia	Bosnia-Herzegovina	Armenia
China	Croatia	Azerbaijan
Fiji	Czech Republic	Bahrain
Indonesia	Denmark	Georgia
Japan	Estonia	India
Kazakhstan	Greece	Iran
Kiribati	Italy	Iraq
Kyrgystan	Latvia	Israel
Malaysia	Lithuania	Jordan
Myanmar	Macedonia	Kuwait
New Caledonia	Moldova	Lebanon
North Korea	Norway	Oman
Papua New Guinea	Poland	Pakistan
Philippines	Romania	Qatar
Russia	Serbia and Montenegro	Saudi Arabia
Solomon Islands	Slovakia	Syria
South Korea	Slovenia	Tajikistan
Spratly Islands	Turkey	Turkmenistan
Sri Lanka	Ukraine	United Arab Emirates
Thailand		Uzbekistan
Vanuatu		Yemen
Vietnam		

Western Hemisphere

Argentina  
Bolivia  
Brazil  
Colombia  
Costa Rica  
Cuba  
Dominican Republic  
Ecuador  
El Salvador  
Grenada  
Guatemala  
Haiti  
Honduras  
Jamaica  
Mexico  
Nicaragua  
Panama  
Paraguay  
Peru  
Suriname  
Uruguay  
Venezuela

Africa

Algeria  
Angola  
Djibouti  
Egypt  
Ethiopia  
Ghana  
Kenya  
Liberia  
Libya  
Madagascar  
Namibia  
Nigeria  
Somalia  
South Africa  
Sudan  
Tunisia  
Uganda  
Zaire  
Zimbabwe

